4 – The Identity Reliability Component

Question 4 *When people identify themselves to you, how do you know how reliable their claim of identity is?*

Answer 4 The Identity Reliability Component

The foundational identity certificate is accompanied by other certificates and by an identity quality record. Very little might be revealed to a relying party about the people identified, other than their identity quality information and the fact that the identity certificate has not been revoked. Despite that anonymity, the Identity Reliability Com-ponent establishes accountability.

How Reliable Is That Identity?

Let's say someone sends you a digitally signed message or document, or they use their identity credential to log into your website or to purchase something from you. How do you know whether you can rely upon that identity? How do you know the signer isn't an impostor?

To answer that we must start with the question, "What is identity?"

We know that a proper identity is represented by a digital identity certificate. And we know that identity is proven when the person identified by the certificate demonstrates that he or she has control of the private key that goes with the certificate.

So when someone signs a message or document or authenticates to your web site with that private key, all is cool, right? You can trust that ID, right?

Not so fast!

First of all, do you know how they got that certificate? That is, do you know how they were enrolled? Anyone can get an identity certificate from any of a number of certification authorities attesting that, for example, they are Abraham Lincoln.

That certification authority's root certificate will in all probability be in your computer, so your computer will give you a thumbs-up on that identity. "Yes," your computer will tell you, "you can trust that signature, because the private key goes with the public key that we have signed."

The public key that they have recklessly signed, that is.

Yes, more inauthenticity.

You need a way for your computer to look at a digital signature or a response to a challenge and tell you, "That identity may be relied upon to the following extent: 16 on a scale of 72."

Let's get back to the question, “What is identity?”

Here's the definition of identity as it appears in my book entitled Identity Quality:

> Identity is the mapping of a natural person to a digital representation of that natural person such that the representation is unique in its namespace and may be asserted and attested for purposes of accountability, facilitation of information transfer, communication, transactions, participation in community, and organizational or business processes.

We use the term “natural person” because in the U.S. and some other jurisdictions a “person” can be a corporation, partnership, or trust. Go figure.

Some PKI folks will note that identity certificates can also refer to objects; to which we Authenticity Alliance folks respond: not in our version of PKI they don't! Objects in our world can have object certificates provided those object certificates are bound to real people holding real identity certificates.

The Authenticity Infrastructure and the Quiet Enjoyment Infrastructure of which it is part adhere to technical standards such as the x.509v3 certificate standard and many others. But where we believe a standard allows or accommodates inauthenticity, we go our own way. For example, the notion that all the information relevant to the reliability of the certificate is in the certificate itself is unworkable.

The Authenticity Infrastructure's credential system starts with your foundational certificate. That's preferably a Digital Birth Certificate but a ReliableID foundational certificate can also serve. The foundational certificate contains the immutable information that is found in your paper birth certificate.

Under normal circumstances that information never changes, and, like the paper birth certificate, the foundational certificate, and its private key are seldom used. Your foundational certificate's private key sits in your home safe or bank deposit box and is used only when you need to sign a certificate signing request for a utility certificate or device certificate. Those are the credentials you'll use on a day-to-day basis.

Your utility and device certificates have normal expirations, and if compromised they may be revoked with a manageable level of hassle and disruption, because you can always go back to your foundational certificate's private key to sign a new certificate signing request.

So you have a permanent foundational certificate as well as transitory utility and device certificates and perhaps an encryption certificate as well. That's still not the end of the credential story; even the attributes of a transitory certificate change over time.

The reliability of a credential is affected by eight things, and a record is needed to tell your relying parties how reliable your credential is in each of those eight metrics. That way, when someone sends you a signed message or file, or when you meet someone in an online network, you have a means of knowing the extent to which you can rely upon their claimed identity as represented by their certificate.

That's what the Identity Quality Assurance measurement system of The Authenticity Infrastructure is all about.

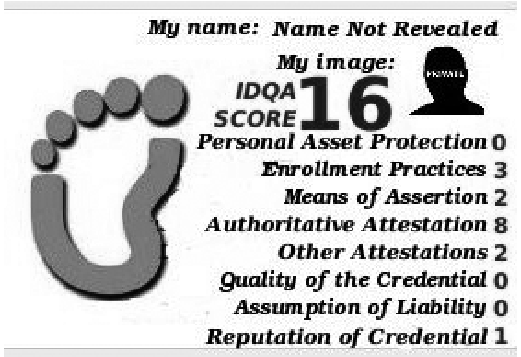
While the underlying foundational identity certificate attests to information that doesn't change, and the utility and device certificates seldom change, the corresponding IDQA score is subject to continual update. Initial IDQA scores and updates to them are digitally signed by Attestation Officers.

An IDQA score is the sum of eight digits, each of which represents the score on a particular "dimension" of identity quality. Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating. Thus the highest quality ID will carry a score of 72. With that one you can buy an office building on another continent while sitting in your den.

This quantification of identity quality answers concerns of enterprises that need to know the costs and benefits of a particular enrollment program.

A note about face-to-face enrollments, which I've noted involve an oath and affidavit: In executing an affidavit, many jurisdictions offer the choice of an oath, which invokes a supreme being, or an affirmation.

Some jurisdictions will not honor an affidavit that was executed using an affirmation-based notarial procedure, and so we use the oath instead. Also, we believe that those who are empowered to apply public authority ought to acknowledge a higher authority. If you claim not to believe in a supreme being, you can swear an oath to That Which Created Me. The phrase "That Which Created Me" can refer to nothing more than an evolutionary process if that fits your belief. That should also work for adherents of faiths that prohibit invoking the name of the supreme being in such procedures.



My name: Name Not Revealed

My image:

IDQA SCORE 16

Personal Asset Protection	0
Enrollment Practices	3
Means of Assertion	2
Authoritative Attestation	8
Other Attestations	2
Quality of the Credential	0
Assumption of Liability	0
Reputation of Credential	1

Going back to the original question, if someone sends you a digitally signed message or document, or they use their identity credential to log into your website or to purchase something from you, how do you know whether you can rely upon that identity? How do you know the signer isn't an impostor?

If the credential complies with the standards of the Authenticity Infrastructure, you'll simply click on the icon that represents the person, as in this illustration. Note that the representation of the identity of an individual gives an IDQA score — and nothing else.

Not even the subject's name or gender!

Now of course we don't recommend entering into a substantial contract with someone without knowing at least their name. On the other hand, for years people have been buying and selling things on eBay knowing nothing but some reputational scores, and it has worked magnificently for the most part. The exception has reared its ugly head when real criminals offer to purchase both the identity of eBay members with high reputational scores and their computers, thereby gaining a highly-rated eBay username and password and the complete set of cookies and LSOs ("flash cookies") that go with it.

There will still be the possibility of such a transaction taking place with an identity credential built upon a foundational digital certificate. But the sellers would have to be willing to give up their complete identity, starting with the information in their paper birth certificates.

With reputational scores backed up by identity credentials built upon foundational digital certificates, we have something truly reliable, something that preserves privacy and anonymity, while giving people a chance to license the use of their personal information with the protections of copyright and secrecy law.

But we're still not done with the personal privacy part of the Authenticity Infrastructure. That's because big companies with big databases and big data mining technologies don't need your name or social security number or any other single index in order to track your every move.

Why do they even want to track your every move? They say they want to understand your habits and preferences and financial status in order to present products and services and political agendas to which you're likely to respond. But that's not all. A look at Stanford University's Persuasive Technology Lab reveals the other reason why big organizations want to track you: to manipulate your perceptions.

If you're like most people you're particularly susceptible to this because you don't think it can be done. You know when people are trying to manipulate your perceptions, and so you don't fall for it, right?

Well, if you've never been fooled by a stage magician, congratulations. You are less vulnerable than the rest of us. But forgive me for not being convinced. Most of us have been fooled by the most elementary sleight-of-hand tricks. Certainly I have.

But all of us form our opinions and outlook on life based upon the information that is presented to us by friends, family, community...and media. So if a captologist wants your soul, he just needs to know the attributes that identify you. He finds those attributes in the trail of fingersteps and unique identifiers you leave in your computer or phone and around the Web.

So let's mess up that trail of fingersteps, shall we?

We'll show how the Personal Information Ownership Component lets you do that, but first we need to protect your formal information and that which is assembled from your fingersteps. We need to look at how it's made vulnerable.

Universality Prevents Sharing of Credentials

Back in the days of the Web it was assumed that a puzzle kit (certificate plus PEN or private key) could be kept as a file on a computer. But that gives rise to other problems. First, anyone using that device after the subject has entered the keystore password can pretend to be the person identified by the certificate. Second, the certificate is only as portable as the device, and people now typically use more than one device. Third, a computer or phone or tablet's operating system is designed to facilitate access to files. Given that environment, and even though operating systems somehow manage to protect private key files, that's just not good enough.

Private files should be kept in a space controlled by a "brain dead operating system," one that knows only how to do the things that its makers want it to do: receive input from a directly attached pinpad or biometric reader, make keys available for encryption and decryption, and perform encryption and decryption. There should be no APIs, no facilities for developers to add features; in fact nothing for developers, period.

The solution is a physical key holder called a "token" or "hard token" You probably already use a token in the form of a bank ATM card. We noted the remarkable fact that the technology in your ATM card is more ancient than the floppy disk, and yet bank ATM networks tend to be more secure than corporate networks. The difference is not one of credential technology; the important difference is a difference of outlook, philosophy, and architecture.

Your bank's ATM network starts with the premise that knowing who you are is the foundation of security. As we pointed out, if authentication on the company network required the use of an ATM card and PIN, people would not share their access credentials.

The reason is very simple: the employer-issued credential protects the employer's resources while the ATM card protects the employee's own money. One is important, while the other is precious. That fact is basic to the design of our solution, the way to deploy tokens in a workable fashion.

Universality is an important goal of our Identity Reliability Component. Universality means two things: universal acceptance of the credential by applications in its user's life, including banking, health care, employment, and shopping; and universality in its deployment around the world.

In order for its user to treat it as though it protects personal assets, it must appear likely to be used in all those applications — if not at the time of issue, then at least in the foreseeable future after enrollment. If the token is seen as just another attempt to secure the company network, it will be shared. It must be positioned as being universal, powerful, and — above all — personal.

Identity in Use Can Be Made Simple

The QEI components discussed in the previous chapters illustrate what goes into the making of identity credentials, a set of processes that may strike you as complicated.

But if the making of credentials seems complicated, wait 'til we start dealing with the complexities of credentials in use!

That shouldn't be surprising when we think about the complexity of identity as manifested in the physical world. You start out life with a paper birth certificate (really a certified copy of your record of birth,) which you keep in a safe place until you need an identity credential for travel (a passport) or an identity credential for driving (a driver's license).

A driver's license is necessary to obtain a motor vehicle registration or to enroll in government programs such as the U.S.'s Social Security. These issue yet another identity credential, a Social Security card. Your driver's license or passport must accompany another credential, a boarding pass, in order for you to travel by air, or to obtain another credential, a health insurance card. Beneath it all is the seldom-used but all-important "breeder" document, the copy of the record of your birth, as certified by public authority.

Another credential consists not of a physical card but rather a collection of data in rows of tables at credit bureaus and retailers and "cookie clubs," aggregators of data about your online habits. That invisible credential has become as essential to everyday life as the driver's license.

Why is it all so complicated? The identity credential is a conceptually simple thing: here is an information object that is bound in a one-to-one relationship with a physical specimen, a human being, evidencing some attributes (name and age and gender) so that the physical person may participate in the physical and non-physical world.

Actually, the use of identity in the online world can be made much simpler than the use of identity in the physical world, to all parties involved. That's not to say that the system will be simple. Under the surface, the collection of moving parts will be as complex as the device that serves as the physical platform — the "wallet" — for the identity.

The phone is the physical platform of choice going forward, as we will almost always have our phone with us. Have phone, assert identity anywhere. Seems simple.

But sometimes we won't have the phone with us. And phones get lost. Phones get stolen. Phones break. Last year's phone gets replaced by a newer phone. Older information appliances (computers and tablets) will not be able to connect to the phone for session authentication. And so we need multiple devices to identify one person. All of them need to be tied to one foundational "breeder" puzzle kit (ID certificate plus PEN.)

Furthermore, the PEN used to sign things should not also be used to decrypt things. Then there's the "Mobil Speedpass" consideration, where many, probably most, authentication situations do not require three or even two factor authentication. We wave our Speedpass at the Mobil pump and the simple fact of possession is sufficient for authentication. That means people will need a separate puzzle kit from the four-factor puzzle kit needed for very confidential and valuable documents.

Multiple puzzle kits will inhabit one device. One can easily imagine a dozen or more puzzle kits inside one phone or other device. All of them will be bound to the breeder puzzle kit that the subject keeps safely in a safe deposit box or home safe.

But we're not done with those dozen puzzle kits in one device. Your identity credential will be so important to your life that you can't risk being without it if you don't have a working phone. Other platforms must simultaneously be usable to identify you. Multiply the puzzle kits inside each device by the number of devices and you get… complexity!

It's starting to seem a lot less simple, right?

But stay tuned for a moment.

Life is complex. That phone is hugely complex. Designing and building the modern smartphone and the systems in which it operates must qualify as one of the most complicated undertakings in human history.

Yet some very smart people (thanks, Steve!) worked hard and thought hard about how to squeeze the complexity out of the phone's user experience and cram it back into the recesses of the circuitry and the software and the network and the business arrangements. The result? Every kid can summon the services of that monumentally complex device.

The identity credential can and must be that simple to use. As just one example, there is no need to involve the subject in the choice of puzzle kit for any particular application or relying party, but if a technically-oriented subject does want to be involved, the details must be readily available.

It's time to take inventory of all the requirements of a viable credentialing system. What does it need to accomplish, and what attributes does it need in order to achieve those required goals?

What Are We Trying to Accomplish?

Let's start by looking at some questions that reveal specific needs — the pains to be cured — of individuals and organizations needing reliable identity credentials:

1. I know this signed message is from Alice's computer, but how do I know it's from Alice?
2. I know Bob's computer can decrypt this file, but how do I ensure that only Bob can read it?
3. What good is a national ID card in a world where streams of packets routinely disregard national boundaries?
4. How can I get employees to stop sharing network access passwords and tokens?
5. How do we solve the problems that are inherent in commercial certification authorities?
6. How do I know that the consultants and contractors accessing my company's files are who they say they are?
7. What level of assurance do I have that this consultant logging in to the acquisition data room is who he says he is?
8. How can I relieve my network security people of the time-consuming burden of resetting forgotten passwords?

9. How can I gain the benefit of letting employees protect their own assets with their ID card without my company incurring liabilities?
10. If I use this credential everywhere, what prevents me from being tracked everywhere?
11. How can my hospital comply with the demanding patient and practitioner ID requirements of HIPAA?
12. How can my financial-services firm meet demand for single-sign-on access to multiple services?
13. How can I reduce all my cards and all my passwords to one, and be more secure as a result?
14. How can we control access to our buildings and our network with one card and one enrollment database?

In order to address all of those needs, our Authenticity Infrastructure will need to have the following attributes:

1. Validity: The credential must provide access to the services of multiple relying parties.
2. Stringency: Issuance of the credential can occur only after procedures appropriate to its level of Enrollment Quality take place.
3. Auditability: The owner, the subject of the identity, must be able to prove at any time that the credential was properly issued.
4. Recourse 1: If I am injured by some anonymous user there must be a means of redress.
5. Recourse 2: In a high-value transaction or other important reliance on a claim of identity, a bond must be available in case the identity claim is fraudulent.
6. Recourse 3: Attestation professionals must carry civil and criminal liability for their work. They must be bondable, insurable, and subject to laws governing the actions of public officials.
7. Reliability: A relying party must be able to quickly discern the reliability of a claim of identity.
8. Universality: Licensed independent attestation professionals carrying public authority must be available in almost any jurisdiction in the world.
9. Built-in insurance against misuse: The credential must be designed to protect subject's personal assets, not just employer assets.
10. Simplicity: As much as possible, the credential must fit the way people live rather than requiring major changes in their habits.
11. Immutability: The identity credential itself must attest only to permanent birth certificate information, not to a changeable relationship.
12. Adaptability: The credential must be designed to facilitate binding and unbinding of relationships, privileges, responsibilities, and other authorizations as needed.

13. Versatility: The credential must allow any standards-compliant authorization record or access control list or physical door lock to base authorization decisions upon it.
14. Portability: The credential must work with any standards-compliant PKI (employee ID, ATM card, HMO card, etc.).
15. Authority: The certification authority must be operated by a noncommercial standards body with public authority, not by a commercial enterprise.
16. Soundness: The process must be governed by a sound certification practice statement and sound certificate management policies.
17. Resistance to tampering: All approved token technology must pass tamper tests; use of soft credentials must be limited.
18. Flexibility: The user must be able to choose any standards-compliant token: USB fob, smart card, ibutton jewelry, phone MicroSD, or SIM chip.
19. Privacy: Personal information must remain the property of the subject, who sets disclosure policy and controls its disclosure.
20. Economy: The credential must cost no more to issue in batch settings than a typical employee ID, and must cost less to maintain.

Some of the required attributes and features have been around for quite a while, yet still seem easy to overlook. For example, liability and recourse in online transactions are frequently discussed, but solutions never seem to be introduced into the discussion.

Let's look at one remarkable, proven example that shows how inexpensive a reliable identity credential can be, and how reliable an inexpensive identity credential can be.

Separating Foundational Identity from Relationships

One basic element of our Identity Infrastructure is the separation of identity from relationships. This is designed to solve a problem that has plagued existing public key infrastructures: access to their resources is controlled by a key pair that typically represents a relationship between the user and the organization that issued it.

For example, a digital certificate or token is often issued by an employer to grant employees access to company network resources. The power of universality described above shows the advantage to both employer and employees of letting the employees use token-based digital certificates+PENs for purposes not related to employment, such as banking, shopping, or access to controlled-access spaces operated by community groups.

The advantage to the employer is that it increases the importance of the token and helps ensure that the employee will guard the credential and its use. As noted earlier, if bank ATM cards were used for authentication to a company's network, the problem of credential sharing would disappear.

But at the same time employers are concerned about possible liabilities incurred by permitting such broad use of tokens and certificates, and about what happens when an employee's employment ceases.

In an age when online authentication becomes more and more important, the only solution is a token that does not represent any relationship. Rather, it stands by itself, simply attesting to a person's existence and unequivocally identifying the individual, precisely as the traditional birth certificate does. Just as the authority behind a birth certificate is public authority, so it should be with the digital version.

A token whose digital certificate contains only key pairs, issuing authority, and other traditional certificate information plus information taken from the individual's birth certificate, and is compliant with internationally-recognized standards such as the PKCS series of standards, can be used to link with other certificates representing relationships with employers, banks, health care organizations, avocational, civic and professional groups, etc.

Traditional credentials may attest to your identity in terms of your relationship to an organization, institution, or employer: "This person is a current employee of Acme Corp. and is entitled to access to the following parts of Acme's online network." But what happens when that relationship changes? Why, your certificate and token are revoked, of course.

What then happens to your access to other online resources that are part of the same trust network as Acme? Well, they have to check every relevant certificate revocation list in the trust network of which Acme is part. The bigger that trust network grows, the more difficult it is to coordinate and synchronize the activities of all the certificate authorities, registration authorities, certificate revocation lists, and directories of all the organizations and their servers. Those PKI networks were designed to attest not to a person's existence, but to a person's relationship with an organization.

Your Osmio VRD Foundational Certificate is not based upon a relationship. Or rather it is based upon one relationship, the relationship between a name and a human body. Osmio VRD attests to a person's existence. You can change jobs, change residence, change marital status, even become a felon. Your Osmio VRD record is permanent.

It might appear that the driver's license or passport is a credential that is independent of relationships, but neither one really is. They represent transitory relationships with a government and with a domicile.

Identity is best represented by a birth certificate. Everyone knows that the information on a birth certificate never changes, and most people understand why that is important. Just the name Osmio VRD Birth Certificate carries with it a benefit, in that the holder of something called a birth certificate will understand that it's not just another supermarket discount card.

Anyone familiar with identity issues knows that standard birth certificates are notoriously unreliable, as they typically are produced using only the oldest and weakest of paper document authenticity devices, often even lacking a raised seal. Further, every birth and death records office uses a different format and different authenticity devices. Unless you are an identity verifier familiar with birth certificates from every municipality in the world, they are virtually useless.

The unreliability of birth certificates comes only from documentary issues. The integrity of the issuance and records maintenance process is actually quite high in records offices around the world. The X.509-based birth certificate and PEN, stored securely and used only to generate other day-to-day certificate + PEN pairs (puzzle kits) and conveyed in a secure token instead of a piece of paper, will make the birth certificate once again a reliable credential.

If Identity Is the Foundation of Security, then identity needs to be a constant. The foundational identity credential needs to never change, from birth beyond death to estate. Once you have that, you can generate as many utility credentials as you want, and also attach as many relationship credentials to it as you want. And those relationship credentials may be relied upon by as many authorization circumstances as you, or your relying parties, want. But the basic identity credential must be a secure digital certificate and PEN.

While a principal relying party, such as an employer, may pay for the enrollment, the credential is not part of an employment relationship, a customer relationship, or a membership in some organization. A single certification authority attests only to the subject's identity, so there is never any doubt about where to go for the authoritative certification of a particular individual. Separate certificates bound to the utility certificate may attest to relationships. In QEI, the disclosure of any information relating to those certificates is under the complete control of the subject.

Realistic Convenience and Realistic Security

A universal credential must be convenient in the way a soft credential or a single-factor token is convenient. A soft credential's private key resides on your personal computer or other information appliance, ready to spring into action whenever an application calls for it, with no other device required. An example is the ExxonMobil Speedpass, which allows you to touch your key fob to a gasoline pump to complete a transaction, no PIN required. The single factor here is possession.

But let's say the task is to release $10 million held in escrow from a development project. Or let's say you're a judge and a digitally signed request for an emergency search warrant has appeared on the screen of your phone.

Now we need three-factor security, that is, a device that only releases the private key after the user enters a PIN or password and presents a biometric, such as a fingerprint, on the device itself.

How can we accommodate the entire spectrum? It's not as simple as identifying which roles need which level of security. Judges don't want to go through three levels of security every time they buy gas. And everyone from time to time needs to sign documents that require high-level authentication.

Different Puzzle Kits for Different Situations

Let’s look a little more closely at the life of a judge. First thing in the morning, she wants to get a quick look at today's docket. The docket is public information; it can be kept in the reception area of the online court clerk’s office, where single-factor authentication is sufficient. The single-factor key on her phone is all the security needed.

Later that evening, at the theater, the judge’s phone starts vibrating. A police officer has submitted a request for a search warrant. The PEN (private key) that she needs for this task requires three factors: possession, finger or eye biometric, and PIN. She discreetly reads the warrant request, clicks “sign this court order,” runs her finger over the fingerprint reader, and enters her PIN. The signature program in the token is then allowed access to the three-factor private key.

Did you notice a vulnerability? If our judge enter her three-factor PIN on the phone's keypad, that exposes the PIN to the phone's operating system, that is, to the set of software tools given to developers so they can write software that generally takes control of the device.

That is why the three-factor token should not be the phone itself, but rather an SD or SIM chip inside the phone that is connected to a pinpad and fingerprint reader on the back of the phone. At the time of this writing such a design with pinpad and fingerprint reader connected only to the isolated processor is only practical for phones with an appropriate slot, such as an SD card slot, accessible from the outside. Phones such as Motorola's Droid X, whose MicroSD slot is only accessible with the battery door removed, will require some engineering.

Those who are familiar with the popular ARM processors used in many phones might note that newer ARM processors include a second processor called the TrustZone, which is isolated from the main ARM processor and which uses its own isolated memory. Indeed it is possible that some day the TrustZone processor might drive the external pinpad and fingerprint or iris reader, but for now that use is not accommodated in its design.

As of this writing AMD has announced that it will be incorporating TrustZone technology from ARM Holdings into its X86 processors. Perhaps this represents an alternative to TPM.

Another possible platform from which the PEN Component can be implemented is the Trusted Execution Environment from the GlobalPlatform industry consortium. TEE’s Secure Element technology appears to do for mobile phones and their operating systems what TPM does for personal computers.

If our judge does not own a three-factor token that is physically housed in a phone, she can still sign that warrant or other court order with a three-factor USB token that can be plugged into her Android phone, equipped with the signing app.

Each of the one-, two-, and three-factor applications is supported by a different puzzle kit (certificate + PEN) and bound to the foundational certificate that was established at enrollment time.

The idea of multiple key pairs in one device got started in the late ’90s, when a case was made for separate key pairs for encryption and authentication. Later, the Swedish organization Secured Electronic Information in Society (SEIS) advocated the use of three key pairs, one each for encryption, authentication, and signing.

Multiple key pairs (puzzle kits) may seem cumbersome and costly, but they're really quite easily accommodated. Whenever people get a new token, they simply sign a certificate-signing request with their foundational private key. The real overhead is in enrollment, particularly the higher-scored digital birth certificate (notarial, face-to-face) enrollments.

Under normal circumstances that will only be done once for a given subject, until the need arises for a foundational certificate with a higher enrollment quality score. Once that labor-intensive process has been accommodated, dozens of key pairs and other identity-related files can be generated with today’s powerful equipment at very little additional cost.

Use of multiple key pairs can be designed to add little or no complexity for the user. The application and/or the Certification Practice Statement knows what key pair it needs. If it needs the three-factor pair it simply prompts the user for the appropriate action, i.e., “please use the fingerprint reader and enter your three-factor PIN.”

In fact, not all of the identity credentials use asymmetric key pairs. Written onto the token along with the key pairs is a simple serial number, used by an RFID chip that doesn’t even use cryptography for lightweight possession-only authentication, as in the Speedpass process.

Any of the key pairs can be individually replaced if it is compromised, unless circumstances call for a replacement of all of them — such as the compromise of the foundational PEN (private key), which should be kept in a bank safe deposit box.

Here are some of the different puzzle kits (certificates plus PENs) that someone might have:

1. Basic Puzzle Kit: A lightweight puzzle kit supported only by an email address validation process; a “Montaigne” puzzle kit that allows people to start gaining the benefits of QEI in the quickest, easiest way.
2. Foundational Puzzle Kit: A type of puzzle kit generally used to generate signing requests for other puzzle kits. The Foundational Puzzle Kit will be generated by either the ReliableID™ or the Digital Birth Certificate™ enrollment procedures. ReliableID™ uses an online but out-of-band enrollment procedure and results in a lower Enrollment Quality score; the Digital Birth Certificate™ procedure is a notarial, face-to-face process, resulting in a higher Enrollment Quality score. A ReliableID Puzzle Kit may be upgraded to a Digital Birth Certificate Puzzle Kit through the appropriate (re-) enrollment procedure.

The certificate-signing request for a Digital Birth Certificate enrollment is signed by the Attestation Officer and asserts only the information that is normally found on paper birth certificates: name at birth, date and place of birth, gender, race, parents' names, parents' address(es) at birth. It is accompanied by digital copies of evidence supporting the claim: paper birth certificate, passport, driver's license, etc. At the subject's direction, the evidence files may be securely escrowed by the Attestation Officer in order to prove the validity of the enrollment if it is later challenged, or may be destroyed at the time of enrollment.

1. The Foundational Puzzle Kit's keys are sufficiently long, 2048 or 4096 bits, so that it remains secure through years of processor improvement.
2. The Foundational Puzzle Kit's PEN (private key) is to be stored in an encrypted thumb drive or encrypted on a DVD and kept in a bank safe- deposit box or home safe. The encryption password or passphrase should be something you are sure to remember. To provide for events that may leave you incapacitated (may be a euphemism for "dead") you should share the PEN and its encryption password with someone you trust. Your Attestation Officer will provide foundational PEN escrow for a fee.
3. ReliableID Puzzle Kit: A Foundational Puzzle Kit established via remote out-of-band enrollment procedures, as opposed to the notarial face-to-face procedures of the Digital Birth Certificate enrollment.
4. N-factor Device Puzzle Kit: This certificate plus PEN is bound to a specific device and attests to the use of a specific set of identity factors, e.g. possession, PIN, fingerprint.
5. One or more low-security identifiers, to be used in single-factor authentication situations such as the Mobil Speedpass application, where the value of the communication or transaction is low. This is actually not a key pair but rather a simple serial number, which if compromised may be overwritten through the use of the Osmio VRD Foundational PEN. In other words, if you have lost one of your wallets you may change your single-factor key so that it cannot be used by someone else.
6. One or more two-factor puzzle kits, where possession plus either password (PIN) or an on-token biometric such as a fingerprint is required to permit use of the private key.
7. One or more three-factor puzzle kits, with escrowed PENs (private keys) for applications requiring highest security. In this case you will need possession, password, and biometric every time you want to use the token. This is the key pair that should be used for your workstation, in conjunction with proximity features such as that in your Osmio VRD Wallet, so that if you walk away the screen will blank.
8. An encryption-only puzzle kit, not to be used for signatures or authentication.
9. An authentication-only puzzle kit, not to be used for encryption or signing.

10. A signature-only puzzle kit, not to be used for encryption or authentication.
11. A PGP key pair.
12. A two-party key pair. The PEN (private key) in the pair is only released for use when an Attestation Officer concurrently presents an Osmio VRD Signing Key Pair. (Recall that notarization is about more than attesting to identity; a notary also attests that your act does not appear to be coerced, that you understand what you are doing, and that you are not inebriated or otherwise incapacitated.) This might be called **four-factor authentication**, the four factors being
    - Something you have (Osmio VRD Wallet)
    - Something you know (PIN, password or passphrase)
    - Something you are (thumbprint)
    - A competent witness's attestation (Attestation Officer's signature)

For the fourth factor to constitute a notarial act, including among other benefits the invoking of the penalty of perjury, the Attestation Officer must be in the physical presence of the subject at the time of signing, and there must be a paper counterpart to the document.

13. One or more non-escrowed puzzle kits with non-escrowed PENs. Actually all puzzle kits created in most of the world fit this category, provided the subject has not chosen to have PENs escrowed by an Attestation Officer for safekeeping. Non-escrowed PENs are mentioned as a separate category because they are illegal in parts of the world. Subjects will not be able to use these pairs in jurisdictions where non-escrowed keys are illegal.

If the subject loses the wallet or forgets a non-escrowed pair's password, anything that has been encrypted with its public key is gone. There will be no way to ever recover the information.

This is the only situation that will accommodate a key pair that is generated on the token itself.

1. Rental Credential: A puzzle kit that is bound to your Foundational Certificate for a short period of time and is then bound to someone else's Foundational Certificate. The times and foundational public keys of the bindings are kept in a secure database, retrievable only upon receipt of a court order or at the signed direction of the subject. The Rental Credential represents another means of providing accountability to relying parties while preserving the subject's anonymity or pseudonymity.
2. One or more puzzle kits related to employment or other relationships with organizations, which require PEN to be exported. Normally, PENs are never exported from the wallet in QEI.
3. Other key pairs may also be placed in the Osmio VRD Wallet:

- Puzzle kits for dependents, that is, minors or others who are not able to act legally on their own behalf. These key pairs may be exported (as when a child reaches the age of majority) or imported (as when an elderly person becomes unable to act legally on his or her own behalf.) Dependents should have their own records in the Osmio VRD database, that is, they need to go through the enrollment process even though they will not be issued an Osmio VRD Wallet.
- Puzzle kits for executors of estates of deceased persons.
- Puzzle kits for people in witness-protection programs and intelligence agencies, for purposes that are exceptions to the principle that authenticated aliases are bad. There is no provision for this in the current Osmio VRD Certification Practice Statement, which will need to be modified to accommodate it.

Each of these key pairs, as well as the simple identity number, will need a name. This will avoid the problem with Symantec's VeriSign certificates, where the fact that they're all called by the same name confuses the large number of users who do not know about the different levels of VeriSign certificates.

In many cases users may choose which key pair they want to use for a particular situation. For instance, one person may only want a single factor to open the door to a home or start a car, while another might want two.

Measuring the Quality of an Identity

Identity Quality Assurance is a methodology for assuring that an identity assertion (credential plus identity infrastructure) is appropriate, as measured in each of eight categories, for access to and privileges in the specific digital and/or physical assets or procedures that use it.

The eight categories or "dimensions" by which IDQA measures identity quality are

1. Degree to Which the Identity Protects Personal Assets
2. Quality of Enrollment Practices
3. Quality of Means of Assertion
4. Quality of Authoritative Attestation
5. Quality of Other Attestations
6. Quality of the Credential
7. Degree of Assumption of Liability
8. Reputation of the Credential

Identities and Identity Management are two different things. Know the quality, and therefore the reliability, of the identities in your system. Is the Identity Quality of each one appropriate to its current and planned application?

The Eight Dimensions of Identity Quality

Degree of Protection of Personal Assets. Does the user have "skin in the game" or are the organization's assets the only ones at risk? If the only reliable way to prevent credential sharing is with credentials that protect the user's financial, reputational, and identity assets, then to what extent does the identity protect those personal assets? Ownership of the credential by the subject is considered part of this criterion, as the credential itself should be a valuable personal asset.

Quality of Enrollment Practices. What type of enrollment procedure was used? Did it involve PII corroboration ("KBA")? Was it face-to-face notarial or remote? How is provisioning performed? How is the process supervised and audited? How many eyes are watching? Each risk profile and highest protected digital asset value will call for a particular enrollment procedure.

Quality of Means of Assertion. Does the credential support OpenID, i-Name, Shibboleth, CardSpace? Does it use SAML assertions? A well-used identity is a more reliable identity; the more places it is used, the better.

Quality of Authoritative Attestation. Who attests to the validity of the assertion, that is, the claimed identity? Is the attesting party a certification authority? How reliable are its attestation practices? How is identity status reported: CRL or OCSP or another method?

Quality of Other Attestations. To what extent do colleagues of the subject corroborate the subject's claim of identity? The more acquaintances willing to put their own identity quality scores at risk, and the higher those scores are, the higher this score will be.

Quality of the Credential. What are the characteristics of the credential and its carrier? Is one key pair used for everything, or are different key pairs or simple serial numbers used for different applications? The carrier of the credential is equally important. Some risk profile/asset value situations call for two-, three-, or four-factor hardware tokens, or a one-time password, while for others a soft credential in the client computer or even a record in a directory will suffice.

Quality of Assumption of Liability. If fraud is committed with the use of the credential, who carries the liability? Is that commitment bonded? What are the terms of the bond? What is the source of funds for fulfillment of the bond? Are there caveats or is the commitment absolute, regardless of the circumstances that made the credential available to the perpetrator? To protect assets and processes of the highest value, where a compromised identity would have the most serious consequences, there should be both civil and criminal liability involved in the issuance and ongoing use of the credential. Equally important is protection against fraudulent repudiation. Nonrepudiation is perhaps the most difficult goal for a trust system to achieve, but it is necessary for the system to be useful to relying parties where significant transactions are involved.

Reputation of the Credential. How long has the credential been used without revocation or reported compromise? How many transactions and authentication events has it been used for in total? The longer a credential has been used without incident, the more reliable it tends to be. Note that the reputation of the credential is not the same thing as the reputation of the subject. For example, if a subject with a very good reputation has a habit of lending his or her credential to family members and colleagues, resulting in documented confusion over who is responsible for what, then the reputation of the credential is greatly diminished.

Each of the eight Dimensions of Identity Quality is measured using a scale of 0 to 9, with 0 being the lowest rating in a particular dimension.

Aggregate Identity Quality Goes From 0 to 72

Adding all eight dimensions for a particular identity yields a rating between 0 and 72.

To illustrate:

Let's begin by describing the characteristics of a credential with a quality rating of 72, the top quality rating on our scale.

A credential with a rating of 72 is as reliable as an identity credential can be. Full nonrepudiation is supported, with financial liability being held by the holder, the Attestation Officer, and the Attestation Officer's licensing organization. It is a four- factor credential, employing “something you have” (hard token with isolated processor, isolated private keys, isolated PIN entry pad, isolated display, isolated biometric capture, and isolated on-token biometric store), “something you know” (passphrase), “something you are” (on-token fingerprint or iris reader), and “proof the server knows” (encrypted PassMark-type image that does not exist in the clear anywhere), all contained in a FIPS 140-2-compliant or equivalent physical wallet (hard token). The foundational key pair was generated by an enrollment professional with credentials meeting Tabelio standards, which in turn adopt the identity verification and record-of-integrity standards of the UINL (International Union of the Latin Notariat) using VIVOS-level equipment in a face-to-face setting where four biometrics were captured, encrypted and digitally signed, including facial image and voice captured during the administration of an Oath of Identity, after which the Affidavit of Identity was signed, and the corresponding jurat signed and sealed. The legitimacy of the subject's claim to identity has been attested to by at least 16 colleagues whose own identities represent a total identity quality score of at least 500. The subject has consented to having an escrowed copy of the enrollment records available upon digitally signed request by relying parties who have been given explicit nonrepudiation evidence privileges at the time of a transaction (allowing a relying party to obtain evidence that the transaction was digitally signed by the person who was bound at enrollment time to the key pair used in signing the transaction). Both enrollee and Attestation Officer have put up bonds or escrows of an amount that is suitable to cover the consequences of an act of fraud, and in addition the Attestation Officer is covered by appropriate and adequate errors and omissions insurance. The certification authority that signed the public key of the foundational key pair represents duly constituted public authority; its CRL is updated throughout the day, with OCSP being available at any time. The certification authority assumes financial liability, backed by appropriate insurance, for any and all of its own breaches of its certification practice statement. The identified individual accepts full financial and legal responsibility, backed by a bond the claims against which may be verified online, for any fraudulent use of the credential. The foundational credential may be used to assert identity authority through corporate identity management systems as well as public identity assertion protocols. The credential has been used for thousands of transactions and authentication events over 12 years without incident. Most importantly, the credential protects the personal assets of the holder in addition to any assets of the principal relying party or any other relying parties.

Quality of this identity on our scale of 0 to 72: **72.**

By contrast, the typical identity on a social networking site is completely based upon the user's relationship with the site, which owns and controls the identity (independence value: 0), involved no enrollment procedures other than the filling in of a CGI or javascript form on the site (enrollment quality value: 0), attested only by the enrollee (attestation value: 0), with no means of assertion other than matching of username and password on the site itself (means of assertion quality value: 0), with the credential itself consisting of nothing but username and password (credential quality value: 0), with no liability assumed by anyone in the identity process (liability assumption value: 0) and no meaningful history of reliance on the credential (credential reputation: 0).

Quality of this identity on our scale of 0 to 72: **0.**

One Person, Multiple Linked Credentials

Just as people lose their driver's licenses and passports, they also lose their smart cards, identity tokens, smart phones, and hard drives. There must be, and is, a reliable recovery procedure for each type of loss.

There is always a way to replace those losable driver's licenses and passports, and that way typically starts with the vital records department of a municipality, a state, or province, or a national health service. The original birth certificate is really an entry in a paper database of sorts, an authenticated register of births, kept in the protected archival facilities of an agency of duly constituted public authority where these foundational records of a person's existence cannot get lost. The losable credentials are all logically linked to the non-losable credential in the archives.

So it is with a well-designed system of digital identity credentialing. Such a system is based upon the following:

1. The starting point for any identity credential is the immutable information about the subject's birth. The subject's date, time and place of birth, identity of parents, and other unchanging information is the foundation of all identity assertions;

2. The foundational identity credential is a digital certificate, digitally signed by a certification authority whose identity certification business is not a sideline to a site certificate business;
3. An identity credential that is used for everyday work, commerce, and social networking is vulnerable to loss and theft.

Therefore, the foundational identity credential should take the form of a digital birth certificate and should be used in much the same manner as a paper birth certificate. The digital birth certificate, and its private key or PEN, should be stored in a very safe place and used only for the purpose of generating credentials that are used in everyday life. When one of the latter is lost, stolen, or compromised, or when a new credential in a new form factor is needed, it will be generated using the private key or PEN corresponding to the foundational certificate.

Most of the eight Measures of Identity Quality of any credential are inherited directly from the foundational certificate, ideally a Digital Birth Certificate, that signed the certificate signing request of the utility or device certificate used in the everyday credential. However, the everyday certificates may carry their own IDQA scores. In fact, the Credential Quality score applies only to the actual certificate and the card, token, hard drive, or other device that houses it.

Identity Quality Score Item 1:

Degree of Personal Asset Protection

Value: 0-9

The Personal Asset Protection Score is entered by the Attestation Officer according to the instructions in the Enrollment Order. Verification of access to accounts must be done by means of the subject logging in the presence of an Attestation Officer.

PAP Score Value	Meaning
0	The identity is not "owned" but is simply a username created by the user for access to a particular application or set of applications.
1	The identity was established, and is owned, by a principal relying party, such as an employer, strictly for use in the principal relying party's set of applications and network.
2	The identity was established, and is owned, by an independent enrollment authority only for use in the network of one principal relying party, such as an employer.
3	The identity was established, and is owned, by an independent enrollment authority principally for the benefit of one principal relying party but is available for use elsewhere, or was established, and is owned, by a government entity other than an intelligence agency; is characterized as "user-centric single-sign-on" with ownership not specified.
4	Ownership of the identity is explicitly that of a bank or financial services firm, for use in the accounts with an available cash balance, with the bank or financial services firm as the sole relying party.

5	The identity is owned by a bank or financial services firm, for use in the accounts with an availabale cash balance and also for use in applications and networks of multiple relying parties.
7	Ownership of the identity is explicitly that of the subject, for use in applications and networks of multiple relying parties.
9	The ownership of the identity is explicitly that of the subject, for use in applications and networks of multiple relying parties, at least one of which is a bank or other financial services firm and provides access to an account with an available cash balance.

Alternatively, if none of the conditions above exactly matches the subject's credential and personal asset situation, the Attestation Officer may use the additive-score method by adding the values associated with the following conditions when true (maximum value is 9.)

Add this if	This condition is true
0	The identity is not "owned" but is simply a username that was created by the user for access to a particular application or set of applications.
4	The credential is explicitly owned by the subject.
1	The identity was established, and is owned, by an independent enrollment authority.
2	Ownership of the credential is explicitly that of a bank or financial-services firm.
1	The identity was established, and is owned, by a principal relying party such as an employer.
4	The credential provides access to accounts at a bank or financial-services firm with available cash balances.
5	The credential provides access to accounts at multiple banks or financial services firms with available cash balances in each.

Identity Quality Score Item 2:

Enrollment Practices Score

Value: 0-9

Proper enrollment may take place in an online session where the enrollee is not at the same location where the key pair is generated, or it may take place in a face-to-face setting with a signing agent, notary, Attestation Officer, or other public official. Generally remote enrollment is weaker than face-to-face enrollment. For the purpose of quantifying the strength of enrollment practices, we have assigned a value from 0 to 9 for each of the following enrollment procedures.

Basic Enrollment Procedure

Each procedure begins with the creation of a Basic Certificate. To obtain a Basic Certificate the subject, using a standard Web browser and Internet connection, opens an initial enrollment form that prompts for an email address that is under the control of the subject and to which a validation code can be sent and received. Subject enters a suitable email address and sends a message containing a unique automatically generated validation code. Subject is instructed to check email, open the message with the validation code, and copy the code. The message instructs users to click an accompanying link or to return to the web page from which the email sending process was initiated, verifies that they intended for the enrollment to take place, and pastes the received validation code into the appropriate space in the form, causing the issuance of a Basic Certificate.

REMOTE ENROLLMENT

EPS Value	Meaning
0	No enrollment was performed; there is no claim of identity. The entity that is asserting this identity does not claim that it represents any particular person.
1	The Basic Certificate or other procedure that consists only of simple validation of subject's control of a particular email address.
2	After receiving a Basic Certificate, subject is directed to an Osmio VRD SSL web page. A cookie is placed in the subject's computer; MAC and IP addresses of user's computer are recorded for inclusion in enrollment record; a key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
2	After receiving a Basic Certificate, subject is directed to an Osmio VRD SSL web page that invokes an identity validation session, during which subject is asked a series of questions including national identity number (e.g., SSN in the United States), address of primary residence, driver’s license number, and answers to a series of questions about personal history. Upon satisfactory completion of this PII corroboration session a key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
2	After receiving a Basic Certificate, subject is directed to an Osmio VRD SSL web page. Subject is directed to a web form that prompts for name, address, and identity assertion network ID information, and a telephone number or voip address that the host system calls upon submission of the form. An automated system places the call and an automated voice prompt asks the subject to look for a control number on the computer screen and enter it into the telephone handset. If the correct number is entered, a cookie is placed, and MAC and IP addresses of user's computer are recorded. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
3	Same as preceding enrollment procedure but with the addition of a voice recording step in which the subject is asked to recite a string of digits into the telephone. Each digit is recorded separately in the enrollment record, which is signed by the automated enrollment system.

4	After receiving a Basic Certificate, subject is directed to an Osmio VRD SSL web page where subject fills in a form, including the name of a published information source that lists a telephone number associated with the subject, as in a directory publication, or as disclosed by a principal relying party (employer, insurer, bank, etc.). The Attestation Officer calls the number at a randomly determined time; the subject verifies that he or she authorized the call and enters a one-time web address into his or her browser. The browser presents a control number that subject enters into the telephone handset. If that is done correctly, the Attestation Officer asks the subject a series of questions retrieved from NCMS, ChoicePoint, Lexis Nexis, or other PII corroboration service. If the questions are answered satisfactorily the subject is asked to recite a string of digits into the telephone, and each digit is recorded separately in the database record. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
5	After receiving a Basic Certificate, subject is directed to an Osmio VRD SSL web page where subject fills in a web form that produces an enrollment appointment, including the name of a published information source that lists the telephone number associated with the subject, as in a directory publication, or as disclosed by a principal relying party (employer, insurer, bank, etc.), and username or other identifier for an online videoconference or video chat. At the agreed time the Attestation Officer initiates a video communication with the subject at the published telephone number. The subject answers the phone, verifies that he or she authorized the call, and turns on his or her computer. The MAC and IP addresses of user's computer are recorded, and the subject is asked to enter the control number into the telephone handset. If that is done correctly, the Attestation Officer asks a series of questions retrieved from ChoicePoint, Lexis Nexis, or other PII corroboration service. If the questions are answered satisfactorily the subject is asked to recite a string of digits into the telephone, and each digit is recorded separately in the database record. A key pair and certificate signing request is generated. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
4	After receiving a Basic Certificate, subject is prompted for national identity number (e.g., SSN in the United States), address, driver’s license, and answers to a series of questions about personal history. After satisfactory answering of questions, an Attestation Officer places a telephone or VOIP call to the telephone number listed in subject's name in a public directory or to subject's place of employment at an established organization, asking questions to confirm subject's identity. Satisfactory responses in both online and telephone sessions causes the Attestation Officer to digitally sign an entry at the Osmio VRD Certification Authority authorizing the signing of a ReliableID Level 2 Certificate to the holder of the corresponding Basic Certificate, that is, the subject. Subject is instructed on the creation of a key pair and Certificate Signing Request. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.

6	REMOTELY SUPERVISED FACE-TO-FACE ENROLLMENT (Patent Pending) After receiving a Basic Certificate, subject fills in a web form that prompts for information to be included in an Affidavit of Identity and for preferred times and location(s) for a face-to-face enrollment appointment at either the subject's location or the office of a Notary Public. The resulting affidavit, in the form of a pdf file, is emailed to both the subject and the notary public, who prints the document. At the subsequent enrollment session a computer with video camera and microphone is made to join an online session with a similar computer at the office of an Attestation Officer. The Notary Public uses proper procedures for verifying government-issued identity credentials (driver's license, passport) and birth certificate. (If the birth certificate is not available, that fact is noted in the certificate.) Over the video link, the Attestation Officer asks a series of questions retrieved from ChoicePoint, Lexis Nexis, or other PII corroboration service. If the questions are answered satisfactorily, the Attestation Officer records a video of the subsequent proceedings, in which the Notary Public administers an Oath of Identity, using the affidavit that was previously printed. The video records the signing of the affidavit by the subject and the signing and sealing of the accompanying jurat by the Notary Public. The file is encrypted with the Attestation Officer's key and saved to the Attestation Officer's secure enrollment records database. The Notary Public holds the identity documents to the camera and still images are taken, encrypted, and saved to the secure enrollment records database. If the subject requests an unencrypted copy of the video and still enrollment records, the records are saved to a CD. A digitally signed certification by the Attestation Officer that no other unencrypted copy of the enrollment records exists, nor will the encrypted version be decrypted except under conditions defined by the Subject's Personal Information Ownership Component, is added to the CD, and the CD is sent via certified mail to the subject. A key pair is generated according to the standards defined in this document (Credential Carrier Score). A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database. FACE-TO-FACE ENROLLMENT (Digital Birth Certificate™)

7	After receiving a Basic Certificate, in a subsequent online session, subject completes an Affidavit Form including such information as is typically found on a traditional birth certificate, as well as national identity number (e.g., SSN in the United States), address, driver's license, and answers to a series of questions about personal history. Upon completion of the form, an Affidavit of Identity in the form of a pdf file is sent to subject's email address. Subject prints the Affidavit of Identity and requests an appointment with a Notary Public. Attestation Officer selects a Notary Public meeting QEI standards near subject and makes the appointment. A copy of the Affidavit of Identity may be emailed to the selected Notary Public. Subject then takes this Affidavit and identification documents to the notary, who administers an oath based upon the contents of the Affidavit of Identity and seals the certificate or jurat. Attestation Officer contacts the Notary Public, confirms that verification of documents and oath proceeded satisfactorily, and requests copies of all documents. Attestation Officer digitally signs an entry at the Osmio VRD Certification Authority authorizing the signing of a Digital Birth Certificate to the holder of the corresponding Basic Certificate, that is, the subject. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database. After receiving a Basic Certificate, subject fills in a web form that includes fields for entry of content of an Affidavit of Identity and preferred times for a face-to-face enrollment appointment at the subject's location or the Attestation Officer's office. At the appointment the Attestation Officer, a notary, examines the subject's identity document(s) (driver's license and/or passport); asks the subject a series of questions retrieved from ChoicePoint, Lexis Nexis, or other PII corroboration service; and, if the questions are answered satisfactorily, administers an oath of identity, wherein the subject recites the content of the affidavit. The Attestation Officer signs and seals the jurat attached to the affidavit. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.
8	Digital Birth Certificate (DBC) After receiving a Basic Certificate, subject fills in a web form that includes fields for entry of content of an Affidavit of Identity and a space for preferred times for a face-to-face enrollment appointment at the subject's location or the Attestation Officer's office. At the appointment the Attestation Officer, a signing agent, examines the subject's identity document(s) (driver's license and/or passport); asks a series of questions retrieved from ChoicePoint, Lexis Nexis, or other PII corroboration service; and, if the questions are answered satisfactorily, administers an oath of identity wherein the subject recites the content of the affidavit. The Attestation Officer signs and seals the jurat attached to the affidavit and uses a specially equipped computer to capture biometric data, including fingerprint, iris image, facial image, and voice. A key pair is generated, with one of the keys being designated the public key. The public key, identity-verification supporting information, and any additional Identity Quality information are made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD. The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card, etc.) and recorded with supporting information in the Osmio VRD database.

9	After receiving a Basic Certificate, subject fills in a web form that includes fields for entry of content of an Affidavit of Identity and preferred times for a face-to-face enrollment appointment at the subject's location or the Attestation Officer's office. At the appointment the Attestation Officer, a Tabelio Officer, examines the subject's identity document(s) (driver's license and/or passport) using a source of ultraviolet light that is part of theTabelio Officer's enrollment workstation, compares the documents to examples in the ID Checking Guide, checks the data and barcodes, turns on a video camera with microphone that is connected to theTabelio Officer's enrollment workstation, and administers an oath of identity, wherein the subject recites the content of the affidavit on camera.The Attestation Officer signs and seals the jurat attached to the affidavit and takes a fingerprint and iris image of the subject.The enrollment workstation is used to sign in to an online facility. A key pair is generated, with one of the keys being designated the public key.The public key, identity-verification supporting information, and any additional Identity Quality information is made part of a certificate-signing request, which is sent to Osmio VRD. Subsequently the X.509v3 identity certificate is created by the signing of the public key by Osmio VRD.The certificate is sent to the user's information appliance or wallet (computer, phone, token, smart card etc.) and recorded with supporting information in the Osmio VRD database. The private key is embedded into a fingerprint-enabled USB token, smart card, wireless token, or other multi-factor identity device.The subject is given two copies of a DVD containing all information from the session, including biometric data, encrypted using the subject's key, and is offered an escrow service to safeguard the private key from loss.

Both civil and criminal liability are assumed by the notary in the face-to-face enrollments. While there is also an assurance that that individual is the one named in the identity documents, a fake identity document of particularly high quality is undetectable, and thus it is possible that an impostor's name will be bound to the resulting identity certificate. Even in that case, however, the relying party can be assured of a reliable identity because the public key that is issued and signed is bound inextricably to the human being who was enrolled. If it is subsequently shared in spite of on-token biometrics and other measures to prevent sharing, non-repudiation remains strong.

Identity Quality Score Item 3:
Quality of Means of Assertion Score
Value: 0-5, 8, 9

An Identity Certificate issued by the Osmio VRD may be used without the benefit of an assertion network, or may be presented subsequent to the assertion of an identity via one of the many assertion networks, such as OpenID, Liberty Alliance, or I-Name. The Means of Assertion Score represents the degree of universality of assertion of the identity through the various assertion networks at the time of issuance.

The Means of Assertion Score is applied at time of enrollment and therefore any subsequent changes in available means of assertion will not be reflected in the Means of Assertion Score.

MA Score Value	Meaning
0	Certificate stands by itself and is not associated with an identity from an identity assertion network
1	Assertable only as a username in a single organizational network
2	Assertable only on a single online resource, such as a web site
3	Assertable only through a proprietary group of online resources, such as a group of related Web sites or a federated identity network
4	Assertable through OpenID, CardSpace, or Liberty Alliance
5	Assertable through I-Name
8	Assertable through multiple identity assertion networks
9	Assertable through all current identity assertion networks

Identity Quality Score Item 4:

Quality of Authoritative Attestation (Certification)

Value: 0-9

Score Value	Meaning
0	No certification, no independent IdP
0	Identity provided by traditional IdP after verification-code-do-email procedure or after a transaction-based process with subject
1	Identity provided by IdP using X.509v3 certificate after verification-code-do-email procedure or after a transaction-based process with subject
1	Identity provided by IdP using X.509v3 certificate after verification-code-do-email procedure or after a transaction-based process with subject
1	Identity provided by Basic Certificate (also known as a "stub certificate"), an X.509v3 certificate issued after a simple verification-code-do-email procedure. Can be used as a placeholder for certificate that is to be subsequently issued pursuant to an enrollment procedure.
1	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority via “Level 1” X.509v3 certificate
2	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority via “Level 2” X.509v3 certificate
4	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority via “Level 3” X.509v3 certificate
5	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority via “Level 4” X.509v3 certificate
7	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority with duly constituted public authority via 1024 bit X.509v3 certificate
8	Identity provided by and attested by a WebTrust Audited General Purpose Certification Authority with duly constituted public authority via 2048 bit X.509v3 certificate

Identity Quality Score Item 5:

Quality of Other Attestations

Value: 0-9(max); sum of component scores

The Quality of Other Attestations Score measures the quality of person-to-person attestations that accompany a certificate. Such attestations include OpenPGP or equivalent Web of Trust attestations or other attestations by people who know the subject. This score is additive, that is, the elements of the score are added together to produce the score, truncated to the nearest whole number, with a maximum value of nine.

Score Value	Meaning
0.01	Times IDQA score of attestor for each attestation by an otherwise unqualified PGP Web of Trust colleague Max addition 2.
0.2	For each attestation by a PGP Web of Trust or FOAF colleague
1	Attestation from colleagues with IDQA scores totaling 200
1	Attestation from colleagues with IDQA scores totaling 300, each with a minimum score of 24
2	Attestation of an administrator of an established school system in which the subject is enrolled
2	More than 50 positive feedbacks and over 97% positive feedback rating on subject-owned eBay ID; ownership verified by Attestation Officer
4	Attestation from colleagues with IDQA scores totaling 300 plus attestation from employer or professional association
5	Attestation provided to Attestation Officer from full-time employer of two or more years

Identity Quality Score Item 6:

Credential Quality Score

Value: 0-9

The Credential Quality Score describes the technology used to carry and assert the Subject's identity. It is the known and verified (by the Attestation Officer) least secure means by which the private key corresponding to the IC will be stored. In other words, if the private key resides in both a three-factor hard token and on the hard drive of a typical network-connected computer running a personal computer operating system, then the Credential Carrier Score will be the lower of the two possible values, which in this case is zero or one.

Score Value	Meaning
0	This is used only for credentials that do not use a certificate or the equivalent, such as a certificate that is signed by an ad hoc root CA; the credential is a simple assertion (serial number, url, uri, etc.) with no use of asymmetric cryptography
1	Private key is stored on the hard drive of a network-connected computer running a personal computer operating system without protection from intrusion

2	Private key is stored on the hard drive of a network-connected computer running a personal computer operating system with an intrusion prevention mechanism whose quality has been verified by the Attestation Officer, or in a verified “sandbox” area on a device, such as a mobile phone, but without isolation from the device's general operating system
3	Private key is stored in a verified isolated device with a separate operating environment on a device such as a mobile phone, isolated from the device's general operating system, as verified by the Attestation Officer
4	Private key is stored in a verified isolated device with a separate operating environment on a device such as a mobile phone, isolated from the device's general operating system; all cryptographic operations are performed in the isolated portion of the device, as verified by the Attestation Officer. Use of the private key is enabled by input of passcode from the keypad of the mobile device.
5	Private key is stored in a verified isolated device with a separate operating environment on a device such as a mobile phone, isolated from the device's general operating system; all cryptographic operations are performed in the isolated portion of the device, as verified by the Attestation Officer. Use of the private key is enabled by input of passcode or biometric on the isolated portion of the device and not from the keypad or biometric input of the mobile device.
6	Private key is stored in a verified isolated device with a separate operating system that meets the “Osmium” standard for isolated cryptographic operating systems or an equivalent standard for HSM devices on a device such as a mobile phone, isolated from the device's general operating system; all cryptographic operations are performed in the isolated portion of the device, as verified by the Attestation Officer. Use of the private key is enabled by input of both a passcode and a biometric on the isolated portion of the device and not from the keypad or biometric input of the mobile device.
7	Private key is stored in a verified isolated device with a separate operating system that meets the “Osmium” standard for isolated cryptographic operating systems or an equivalent standard for HSM devices on a device such as a mobile phone, isolated from the device's general operating system; all cryptographic operations are performed in the isolated portion of the device, as verified by the Attestation Officer. Use of the private key is enabled by input of both a passcode and a biometric on the isolated portion of the device and not from the keypad or biometric input of the mobile device. Additionally, the isolated device has a display, circuitry, and Osmium-grade software that is suitable for image verification of a remote facility for authenticity, and a system in which the verification image exists only in encrypted form, with all cleartext versions of the image having been destroyed.
8	A score of 8 may be reached if incrementation warrants, with incrementation by one if multiple key pairs that are separate from an archived foundational private key are used in the establishment and operation of this identity
9	In addition, the CC Code is incremented by two if separate keys pairs are used for signing, authentication, and encryption, with different key pairs used for different types of token usage (single factor, two factor, three factor, four factor), all of which are bound to an archived foundational private key

Identity Quality Score Item 7:

Assumption of Liability Score

Value: 0-9

The Assumption of Liability Score identifies the nature and degree to which one or more identified parties assume liability for the consequences of the use of an identity that was fraudulently obtained.

Score Value	Meaning
0	No assumption of liability by any party
1	Used only for certificates produced by non-notarial enrollment processes. Attestation Officer assumes at least $5,000 liability for the integrity of the enrollment process, meaning that the Attestation Officer takes responsibility for the subject's correct identity.
2	The enrollment was notarial, which means Subject is under penalty of perjury for any false information in oath and affidavit and the enrolling notary (not necessarily the same person as the Attestation Officer) assumes criminal liability against fraudulent enrollment. However, no financial liability is assumed.
3	The enrollment was notarial, and the subject assumes at least $10,000 liability for acts of fraudulent enrollment; however, such liability is not covered by insurance or bond.
4	The enrollment was notarial, and the subject assumes at least $5,000 bonded or insured liability for acts of fraudulent enrollment.
5	The enrollment was notarial; the subject, enrolling notary, and Attestation Officer (if different from enrolling notary) each assumes at least $5,000 bonded or insured liability for acts of fraudulent enrollment.
6	The enrollment was notarial; the subject, enrolling notary, and Attestation Officer (if different from enrolling notary) each assumes at least $25,000 bonded or insured liability for acts of fraudulent enrollment; and the subject assumes at least $100,000 liability, bonded or insured, for any fraudulent act committed with the use of this identity credential or any derivative credential or certificate.
7	The enrollment was notarial; the subject, enrolling notary, and Attestation Officer (if different from enrolling notary) each assumes at least $25,000 bonded or insured liability for acts of fraudulent enrollment; and the subject assumes at least $1 million liability, bonded or insured, for any fraudulent act committed with the use of this identity credential or any derivative credential or certificate.
8	Attestation Officer verifies initially, and at least yearly thereafter, that the subject of the identity certificate carries a bond of $5 million or more that insures the identity of subject and also against fraud in all transactions and events that the subject signs with the identity credential or any derivative credential or certificate.
9	Subject is bonded and the bond applies to any instance where the credential is misused; subject assumes liability for any and all misuse of the credential. Bonding events, including commitments regarding the use of the bond, are signed by the bond issuer and are updated at each bonding or bond usage event, and are made available in an authenticated online space to relying parties.

Identity Quality Score Item 8:
Reputation of the Credential Score
Value: 0-9

The Credential Reputation Score identifies the duration and frequency of usage of the credential without incident, including reports of usage by individuals other than the subject.

Score Value	Meaning
all	Number of years of usage times number of times used divided by 500, to a maximum of 9. The Attestation Officer may adjust this score if there is evidence that the credential has been shared.

Even If There Is Successful Identity Fraud…

Let's suppose that a fraudulent enrollment does take place. The enrollee uses fake identity credentials or, God forbid, the Attestation Officer participates in the fraud.

If the enrollment procedure is of the highest quality, performed by a Tabelio Officer with the biometric capture capabilities of the VIVOS® Enrollment Workstation, then we still have a reliable identity. While we may not know the real name, birthplace, birthdate, and other data that is usually associated with identity, we do know something important: This public key is bound to a human being with this unique set of biometrics. The person who presents the finger, iris, face, and voice that was signed by this key is the person who enrolled at this place on such and such a date. The person is unmistakably identified by the public key associated with that enrollment.

The Left Behind crowd and others who are guided by John Nelson Darby's interpretation of the Book of Revelation will at this point shout in unison, "I told you so!" They may cite this use of the public key as further evidence that we will all be known by a number that is perhaps to be tattooed on our foreheads or right hands, rather than by our given names. This is a little like the notion of the open range Internet crowd insisting that since activity on the information highway is ungovernable, then everything to which the highway connects is beyond the reach of governance. That's only true if human beings voluntarily give up the prerogative to govern that which must be governed.

People will know each other by their numbers only if they choose to do so. Given the length of the public key, that would be highly unlikely even if there were a reason for it, which there is not. Would we remember the number? Of course not, that would be a ridiculous and unnecessary chore. And what reason would there be for someone to wear it visibly on their body?

Who would choose to be known by a number instead of their natural name? Perhaps the official binding between an insurance policy and the person insured will be through a public key, but so what? Insurers, banks, and commercial enterprises in general have identified customers by their account numbers for years. The account holder's natural name will still be on the insurance policy, and the agent who sold it will still know the policyholder by his or her nickname.

We can make fun of the odd branch of evangelicalism that follows Darby's quite novel interpretation of Revelation, but then we have the fact that 60 million copies of the Left Behind books have been sold. My personal feeling is that it is overly prideful to claim to know what such an intractable part of scripture really means, but there are obviously a lot of people out there who truly view things like identity tokens as fulfillment of biblical prophecy. Those same people, however, expect to be whisked away to Heaven, accompanied by every child on Earth under the age of 12, in some instant that will occur before these tokens get deployed. Therefore those who believe that scenario have nothing to worry about. ("We're scheduling employee enrollments next Tuesday." "Sorry, can't make it, I have to catch a flight…")

The rest of us do have something to worry about. Whether it's some nosy government agency or a DoubleClick-type know-everything-about-everyone market manipulator or a megalomaniacal despot or a set of cookie clubs or a network of assemblers or the Beast itself, we must make sure that our new identity tools do not enable anyone to abuse them by improperly aggregating personally identifiable information.

The Personal Information Ownership Component, properly implemented and managed, will protect us from that. DoubleClick will just have to approach us as polite supplicants, explaining in detail just what information they want for what purpose and for how long.

Let's take a look at the Personal Information Ownership Component and the way it at last accomplishes the long-articulated goal of giving each of us personal control over information that identifies us.

To see the current state of development of

The Identity Reliability Component

…and to learn how your

experience with reporting protocols

might be put to use in its development, please go to the Identity Reliability Component Development Office at osmio.ch