3 – The Enrollment Component

Question 3 *How do you establish identity in the first place?*

Answer 3 The Enrollment Component

Enrollment can be costly or not, depending upon the level and categories of rigor need-ed by relying parties. The Enrollment Component ensures that evidence supporting a claim of identity is gathered properly for the requisite level of rigor and presented along with the public key in a certificate signing request to the Osmio Vital Records Department.

If we are to have measurably reliable identities, the enrollment process is obviously important. How does one enroll to gain the benefits of the Authenticity Infrastructure and the rest of the Quiet Enjoyment Infrastructure?

The more rigorous enrollment procedures are performed face-to-face by a signing agent (a specially qualified notary) in most U.S. jurisdictions, or in other jurisdictions by Latin Notaries or their agents, whose enrollment assignments are managed by the licensed enrollment authority.

At enrollment, a key pair is generated. While it could be used right away, ideally that foundational, archival key pair should not be used for authentication but rather should be used to generate other key pairs that are used on a day-to-day basis. But for now, to keep things simple, we'll pretend there is just the one key pair. Later we'll show the many reasons why separate key pairs – puzzle kits – should be used for enrollment records and for day-to-day authentication. Additional key pairs should be used for other purposes as well, but we don't need to go into that now.

The Front Line of Authenticity

An enrollment can be performed either face-to-face in a notarial procedure or remotely, using a variety of "out of band" methods of verifying a claim of identity, where "out of band" refers to the acquisition of evidence of identity from channels other than the channel by which the identity was asserted (claimed). A third method involving only verification of the email address of the subject should be used simply as a first step toward the other two methods, although it does produce a fully functioning identity certificate and PEN. A fourth method takes advantage of recent legislation in the U.S. state of Virginia that allows notarial procedures to take place over a remote video con-nection.

Obviously a face-to-face procedure will yield a higher Enrollment Quality score, but that can be costly in both time and money, and for many purposes remote enrollment will suffice. The Enrollment Quality score of a credential may be upgraded at any time by means of a higher-quality enrollment procedure. That would not be possible if the Enrollment Quality score were stored in the certificate itself, which is one of the reasons that is not the case.

The Enrollment Component calls for four general categories of enrollment procedure:

1. Basic Enrollment Procedure: Email verification only
2. ReliableID Enrollment Procedures: Out-of-band remote verification of identity
3. Digital Birth Certificate Enrollment Procedures: Face-to-face enrollment by a public official
4. "Virginia DBC" Enrollment Procedures: Enrollment by a Virginia notary via video

Within the four categories are further subdivisions reflecting different levels of rigor and different resulting Quality of Enrollment Practices scores to be recorded in the subject's identity-quality record.

The ReliableID and Digital Birth Certificate enrollment procedures produce Foundational Identity Certificates and their corresponding PENs. You'll recall that a certificate and its corresponding PEN constitute a puzzle kit; the Foundational Certificate and its PEN constitute a Foundational Puzzle Kit.

The Foundational Puzzle Kit may be used for day-to-day authentication, but it's much better if it is used in a manner that preserves all the benefits of QEI, including accountable anonymity. Since a Foundational Certificate includes your name and other personal information, presenting it for online authentication is like having someone make a copy of your paper birth certificate when you use it as evidence of identity.

Instead, the Foundational Puzzle Kit is designed to be the "breeder" puzzle kit, kept in a safe or safe-deposit box and only used to generate certificates that are embedded in smart cards, tokens, and phone microSD or SIM chips. Since they are chained to the Foundational Certificate, such day-to-day certificates are called "Chained Certificates."

In each case a key pair is generated, and the public key is sent to the Osmio Vital Records Department, along with the evidence supporting the identity claim. Together those items constitute a certificate signing request (CSR).

Some Enrollment Use Cases

The Basic Enrollment Procedure involves a simple verification of control of an email address in a manner that will be familiar to most users of email and the Web. It produces the very lowest level certificate, the Basic Identity Certificate.

The Basic Identity Certificate is free, and may be used for undemanding authentication and signing purposes. As its name implies, the Basic certificate is intended as a step toward a higher-quality set of certificates, all of which are based on the subject's foundational certificate.

In most cases enrollments will be sponsored, that is, paid for by an employer or an organization with which the subject has a relationship. The sponsor is called the "principal relying party." Let's say the principal relying party is the operator of an online "data room" where information about the acquisition of one company by another is being exchanged. The information would be of great value to securities speculators, competitors, or rival bidders, so ensuring that those who touch it are who they claim to be is of high value to all parties. The operator of the data room will have no problem paying for face-to-face notarial enrollments with a high Enrollment Quality score.

Parents and caregivers of children also have a strong need to ensure that there are online social spaces where the age and gender of participants is reliably known, where an adult predator cannot claim to be a child. But this group will need a more affordable enrollment procedure, so for its members, attestations by school officials may be used. Attestation by school officials may be part of the Other Attestations score if it is not done at time of enrollment.

Remote out-of-band enrollments will suffice for large numbers of subjects and their relying parties. These involve things like "PII corroboration," where a service with access to the rather nosy databases of the credit bureaus asks the subject a series of question that only the identified person would be able to answer correctly. These procedures have been used with success by consumer lenders for years. Automated or human calls may be made to phone numbers listed for the subjects in public directories. A variety of services provided by Authentify, Inc., are useful for this purpose.

The mid-range face-to-face notarial enrollments may be based upon an affidavit of identity familiar to any notary public; the corresponding oath may thus be administered by any notary.

A higher level of face-to-face enrollment will be performed by a notary public who has also qualified as an Attestation Officer. The highest level of face-to-face enrollment will be performed directly by, or under the supervision of, a Tabelio Officer, that is, a specially qualified Attestation Officer, whose legal status as a Latin Notary is supplemented by training on a VIVOS® Workstation, which captures and digitally signs a voice video of the oath, as well as finger, iris and hand biometrics. The video and biometric files are also digitally signed by the Tabelio Officer, who supervises the generating of the foundational key pair and any other key pairs desired, and submits a signed certificate signing request to the Osmio Vital Records Department. The Tabelio Officer also provides complete Osmio VRD credentials, including USB tokens, ID jewelry, MicroSD or SIM tokens for phones, and the Audrey credential. For this service the Tabelio Officer will charge a substantial fee.

For complete details of all the enrollment procedures, see Appendix A.

Liability

A big unanswered question in many PKI schemes concerns liability. Who is financially and criminally responsible for fraudulent enrollments?

First, a qualification. If a candidate for enrollment presents a fake passport of KGB quality, and has been professionally coached on the background of the person whose identity he is assuming, all bets are off. He is likely to slip through, and the Attestation Officer will not be liable for the consequences.

However, a subject who goes to that much trouble must be assumed to have some important business with some relying parties, and in those situations it will be expected that the credential have a high Assumption of Liability score, so that the consequences of fraudulent identity are covered by a bond.

The subject of high-quality fraudulent identity brings with it the discussion of solutions, which include biometrics. If a subject enrolls through one of the top-enrollment-quality Digital Birth Certificate procedures, biometric information is captured. Normally that information is encrypted and sealed away in the subject's safe-deposit box, inaccessible to anyone but the subject.

Still, there will be times when a subject wants the biometric enrollment information to be accessible by relying parties, as stipulated in the subject's PersonalNDA and License (explained later). In such a case, biometric information, even when stored in one of the "encoded" forms that biometric companies like to promote, can be compared forensically with millions of other biometric records, as police departments and national security agencies do with biometrics of convicted criminals. It also can be copied and used by someone else for fraudulent authentication.

If you have no criminal record, your biometric data should not be kept anywhere but in your bank safe-deposit box or home safe. If you do have a criminal record… good luck!

Let's say the user of a fraudulent identity manages to get himself a criminal record. When that happens we will have an iris scan and fingerprint of a known identity fraud perpetrator. Should new enrollees have their biometric data subject to comparison with a database of biometric records of such known impostors? If so, strong assurances would need to be given that the new enrollee's biometric data will never be kept anywhere after the database check is made. If that can be made we will have a database of individuals who will never again be able to enroll anywhere on Earth.

In the meantime, the fraud will go undetected. We can take some comfort in the fact that fake IDs of that caliber are rare, and usually not worth doing because bonding will be expected and difficult to obtain.

However, Attestation Officers who through their own negligence permit a fraudulent enrollment will be financially liable for the consequences. Of course, even the slightest collusion on the part of the Attestation Officer will mean criminal liability as well. That's one of the benefits of ensuring that all Attestation Officers are public officials.

The distinction between detectable and undetectable identity fraud at the time of enrollment will surely be difficult to determine in some cases, and will be tested in the courts and elsewhere.

The Council of Attestation Officers

The existence of standards for those who issue credentials does not get the issuance done. After the standards are set, someone must qualify, recruit, train, equip, and supervise those who actually engage in the practice of enrollment. That is the job of the Council of Attestation Officers.

The charter of the Council of Attestation Officers is to manage enrollment assignments in such a manner that they can make a good living in this very important new profession. Only individuals who are recommended after passing qualifying examinations may be so licensed.

The Council of Attestation Officers will select, train, equip, and license qualified individuals to examine evidence supporting a claim of identity either in a face-to-face notarial setting (they are all notaries with the Signing Officer designation or its equivalent) or via a remote out-of-band procedure; supervise the generation of key pairs; and issue certificate signing requests to the City of Osmio Vital Records Department. In addition, they may be asked by subjects to serve as trusted escrow agents for foundational keys and biometric data, and they may supervise the generation of chained certificates.

If you are a Notary Signing Agent in the United States, or a notary public elsewhere, with a demonstrable track record of integrity, go to http://attestation.pro to learn more.

(E&O)^2

The shorthand name for the process of authenticating the identity of individuals is (E&O)2. or, (E&O) times (E&O).

The first E&O is about a source of trust of the authenticator. Those who deal with financial transactions are familiar with the term E&O, which is short for **Errors and Omissions** Insurance.

Errors and Omissions insurance coverage of individuals in the practice of their profession is significant. It means that an insurance company considers the party to be sufficiently trustworthy for it to assume financial responsibility for certain risks that are part of the effective performance of their duties. When assessing the trustworthiness of an individual being considered for a responsible position, E&O, along with bonding, is a good sign. In fact it is a requirement for our enrollment professionals.

The second E&O stands for **Eyeball and Oath**. That's shorthand for the fact that in a Tabelio Digital Birth Certificate enrollment (face-to-face), a biometric record of the candidate for enrollment is taken, including an iris scan, fingerprint, voice, and video image. The video image is also part of the "O," that is, the oath. The candidate recites an oath of identity into the same camera that takes the iris scan.

“Eyeball” means that we have an iris scan establishing precisely which biological specimen claims to be John Smith, supplemented by a fingerprint and a signed and stamped video clip of the individual, with his voice.

“Oath” means that the person with those biometric characteristics has stated under penalty of perjury that his name is John Smith.

While it is conceivable that a suicide bomber would lie under oath[65] in such a permanent record, would anyone else? The perjury trial would be very short: “Here you are swearing that you are John Smith and here is the irrefutable evidence that you are not John Smith, all in one convenient time-stamped, location-stamped digitally signed file. Case closed, off to jail.”

The second E&O establishes the credibility of the authentication independently of the professionalism of the authenticator.

Overview of All Enrollment Processes

I. Basic Identity Certificate Issuance

The Basic Identity Certificate was originally conceived as the starting point for ReliableID and DBC enrollments; however, it can be accepted for authentication by a relying party whose security requirements are not very demanding. Following is the procedure for generating a Basic Certificate:

1. Through blog PR, bannering, or other outreach method, the subject learns of the benefits of obtaining a Privacy PEN®.
2. The subject clicks a link to a landing page that expands upon the benefits and explains what a Privacy PEN® is, noting that it is what is often erroneously called a digital certificate. Difference between cert and PEN® explained. (“A certificate and the pen used to sign it are not the same thing, right? We'll try to straighten out the language of this remarkable thing called PKI for you, because PKI is too good, too important not to be explained using language that makes sense.”)
3. The subject enters his or her email address in an input box on the landing page and clicks "Get My Privacy PEN®."
4. A link to a key generation page is sent to the email address.
5. The subject clicks the link and is sent to the key generation page. The key generation page should check for a cookie or some other evidence that the user is at the computer to which the link was sent. (This step can wait if necessary.)
6. The subject's computer is directed to generate a 102- bit or 2048-bit RSA key pair. One of the keys is designated the public key and is included in a Certificate Signing Request, which is sent to the Osmio VRD certification authority.
7. The Basic Identity Certificate and its associated PEN® is installed in the key store of the Subject's computer, tablet or phone.

[65] An oath, as opposed to an affirmation, ends with the words, “so help me God.” In some jurisdictions an affirmation does not subject the affiant to penalties of perjury; and the reference to God may actually be meaningful to that suicidal terrorist. For those reasons an oath rather than an affirmation is used.

II. Foundational Identity Certificate Issuance

An Overview of ReliableID and Digital Birth Certificate Enrollment Procedures

1. The subject chooses either on his or her own, or at the direction of a sponsoring organization, the type of enrollment desired. The subject fills out the corresponding enrollment appointment request with required information on the Osmio VRD website.

<u>ReliableID Precedures for Enrollments with Enrollment Practices Score of 2 or 3</u>

1. If the subject chooses an enrollment method with Enrollment Practice Score 2 or 3, the enrollment takes place immediately from the subject's current location. For enrollments with higher Enrollment Practice Scores, an appointment request is generated. For enrollments with Enrollment Practice Scores 6-9 (Digital Birth Certificate™), the subject additionally fills in an affidavit form, which generates an Affidavit with accompanying Jurat in pdf form. The form is sent via email to the subject and to the Attestation Officer whose availability fits the requested appointment place and time.
2. For enrollments that are to generate an Enrollment Practice Score of 2 or 3, the subject uses the Basic Identity Certificate to log in to the ReliableID Enrollment Request site, which offers a choice of unsupervised online validation procedures (depending upon whether the resulting Enrollment Practice Score is to be a 2 or 3). These include entry of a validation code from the computer screen into a telephone keypad and, in jurisdictions where it is available, answering KBA (knowledge based authentication) questions provided by a KBA service. KBA presents multiple choice questions to subject with correct answer taken from credit bureau database.

<u>ReliableID Precedures For Enrollments with Enrollment Practices Score of 4 or 5</u>

3. For enrollments that are to generate an Enrollment Practice Score of 4 or 5, the subject uses the Basic Identity Certificate to log in to the ReliableID Enrollment Request site, which offers a choice supervised online validation procedures (depending upon whether the resulting Enrollment Practice Score is to be a 4 or 5). Subsequently, the subject is called by an Attestation Officer at subject's place of employment or at a telephone number that is listed in subject's name in a published directory. After the call is successfully placed, the Attestation Officer performs a telephone supervised version of the procedure used with Enrollment Practice Scores 2 or 3 above, where the subject is directed to enter a validation code from the computer screen into a telephone keypad and, in jurisdictions where it is available, answering KBA (knowledge based authentication) questions provided by a KBA service.

“Virginia” Digital Birth Certificate Procedure for Enrollments with Enrollment Practices Score of 5

4. For enrollments that are to generate an Enrollment Practice Score of 5, the subject uses the Basic Identity Certificate to log in to the Digital Birth Certificate Procedure site, where the subject fills in an affidavit form, the completion of which generates an Affidavit with accompanying Jurat in pdf form, as well as an appointment request. The resulting form is sent via email to the subject and to the Attestation Officer whose availability fits the requested appointment place and time. The actual enrollment in this case takes place over an audio-video link, as enabled by a law passed by the Commonwealth of Virginia in July, 2012.

Digital Birth Certificate Procedure for Enrollments with Enrollment Practices Score of 6 or higher

5. For enrollments that are to generate an Enrollment Practice Score of 6 or higher, the subject uses the Basic Identity Certificate to log in to the Digital Birth Certificate Procedure site, where the subject fills in an affidavit form, the completion of which generates an Affidavit with accompanying Jurat in pdf form as well as an appointment request. The resulting form is sent via email to the subject and to the Attestation Officer whose availability fits the requested appointment place and time.
6. The subject and Attestation Officer meet at the appointed time. The Attestation Officer asks the subject to recite an oath based upon the contents of the affidavit form. For enrollment practices scores 7 or higher, the Attestation Officer performs a video recording of the oath recital. For enrollment practices scores of 8 or higher, the Attestation Officer must have the additional title and certification of a Tabelio Officer. The Tabelio Officer takes iris and fingerprint biometric data from the subject. The subject signs the affidavit and the Attestation Officer signs and seals the accompanying jurat.
7. After successful performance of the remote or notarial (face-to-face) enrollment process, the subject, under the supervision of the Attestation Officer or of a set of instructions on the unsupervised enrollment web page, generates a 1024- or 2048-bit key pair and Certificate Signing Request (CSR) and sends it to the Osmio VRD certification authority. If all is in order, the Osmio VRD certification authority causes the public key of the pair to be signed by the Osmio VRD Certification Authority Server.
8. In the case of Digital Birth Certificate enrollments, the Attestation Officer supervises the encryption of all data gathered using the subject's new public key and the erasure of the original plaintext version of the data. The Attestation Officer offers the subject the option of allowing the Attestation Officer to keep an escrow copy of the data for extra safekeeping.

9. If the impost fees have not been previously paid by the sponsoring organization, the subject pays the fees.
10. The Osmio VRD may sign and issue the certificate to the subject or, should the application be rejected, the Osmio VRD alerts the subject that the application has been unsuccessful.
11. The Attestation Officer instructs or assists the subject in generating one or more Chained Identity Certificates, and instructs the subject to store the private key and enrollment data of the Foundational IC in a secure place, such as a bank safe deposit box or a home or office safe.
12. Renewal is conducted as per the procedures outlined in the CPS and the official Osmio VRD websites.
13. Revocation is conducted as per the procedures outlined in the CPS.

III. Chained Identity Certificate Issuance

A Chained Identity Certificate is bound to, and issued subsequent to the issuance of, a Foundational Identity Certificate as described above. A Chained Identity Certificate is also bound to a particular device from which it is to be used. The device's design should be such that the PEN (private key) of a Chained Identity Certificate is not retrievable once it has been embedded in the device.

1. The subject generates a 1024- or 2048-bit key pair in his or her computer.
2. The subject generates a Chained IC Certificate Signing Request using the PEN® (private key) of his or her Foundational IC.
3. If a higher Attestation Quality score is desired, the subject arranges for the Attestation Officer to additionally sign the Chained IC Certificate Signing Request.
4. The Certificate Signing Request (CSR) is sent to the Osmio VRD certification authority. If all is in order, the Osmio VRD certification authority causes the public key of the pair to be signed by the Osmio VRD Certification Authority Server.
5. The Osmio VRD may sign and issue the certificate to the subject or, should the application be rejected, the Osmio VRD alerts the subject that the application has been unsuccessful.

I. ReliableID™ Enrollment in More Detail

ReliableID™ Enrollment procedures may be automated or may be mediated by an Attestation Officer, but in any event they are performed remotely rather than in a face-to-face setting. They therefore do not carry the same legal significance as a Digital Birth Certificate Enrollment. ReliableID™ is less costly and more convenient than Digital Birth Certificate.

ReliableID enrollment procedures begin with "out of band" identity verification services that originate with the Authenticity Enterprise named Reliable Identities, Inc., or with other providers of such services including Authentify, Jumio, StrikeForce and

ID Verify, and “dynamic knowledge based authentication” (DKBA) services from RSA, IDology, Lexis-Nexis and others. At the simplest level, a secret is sent via SMS text message to the subject’s mobile phone number. With DKBA, the subject is asked multiple choice questions to which only he or she is likely to know the answer. The stronger (and, typically, more expensive) the procedure, the higher the Quality of Enrollment Practices score.

In addition to the automated out-of-band procedures from Authentify and the KBA providers, the higher-scored ReliableID procedures involve a telephone interview between the subject and an Attestation Officer. The interview is initiated with a call to a telephone number listed in the subject's name in a public directory, or a call to the subject's place of employment. The Attestation Officer has some discretion about accepting alternatives in certain situations, as when the subject is neither employed nor has a listed telephone number.

In a mediated session, the Attestation Officer might go through a KBA question-and-answer procedure on the phone, and/or on a Skype video call. On Skype, an image of the subject should be taken, as well as an image of the subject's photo identification credential (driver's license or passport), along with a driver’s license or passport number. These should be made part of the evidence sent with the certificate signing request.

In general, specifications for ReliableID procedures will need the benefit of experience before they become final.

II. Digital Birth Certificate™ Enrollment in More Detail

Digital Birth Certificate™ enrollment procedures must be performed in a face-to-face setting by a public official who is commissioned by the jurisdiction where the enrollment takes place to apply public authority to documents and procedures. Various levels of Digital Birth Certificate enrollment quality correspond with three levels of qualification of the public official performing the enrollment ceremony:

1. ASA: Any Signing Agent or Equivalent

A Signing Agent is a U.S. notary public who has passed an exam that establishes a uniform level of competence among the various jurisdictions. Notary public qualification standards in most other countries are at least up to U.S. Signing Agent standards, so any U.S. Signing Agent or any notary elsewhere may perform the enrollment ceremony to the ASA standard.

Since the notary or other public official performing an ASA enrollment is not equipped and trained to perform any part of the enrollment other than normal identity credential checking and administration of the identity oath, affidavit, and jurat, the ASA enrollment will also include a ReliableID procedure, where the subject will be responsible for providing a computer for generating the key pair and CSR. Unless special arrangements are made, an ASA enrollment will generate only a computer-based identity certificate and PEN, and not a wallet-based identity certificate and PEN. (A wallet is a device such as a smart card, microSD chip with smart card circuitry, or other device that isolates the PEN from the operating software and circuitry of a computer or phone.)

2. Attestation Officer and Tabelio Attestation Officer

An Attestation Officer will be equipped with a VIVOS® Enrollment Workstation and will be trained on its use.

VIVOS Configuration

Hardware and Accessories

1. 15.4” laptop computer with TPM or ARM TrustZone or Global Platform Secure Element
2. video camera, microphone and MicroSD reader/writer built in to laptop
3. UV light source
4. wet signature capture pad
5. ID Checking Guide
6. Smart card reader/writer
7. iButton reader/writer
8. GPS tagger
9. Secure case: Zero Halliburton E4-SI 4" Elite Attache

The Tabelio version of VIVOS will also include M2Sys or equivalent multibiometrics input device

1. fingerprint capture device
2. iris camera
3. hand vein capture device

Wires connecting peripherals will be covered in tamper-evident yellow tape that is printed with the words “Examine for evidence of tampering.”

Software

1. Ubuntu Linux (11.10 or higher)
2. VIVOSworks, a graphical supervisory user interface program that automatically launches as part of the boot process and leads the Attestation Officer through each step of the process, automatically turning on the video recording when the “Oath Recital” button is clicked
3. Java
4. Bouncy Castle crypto library
5. CSRtool, a graphical tool for generating RSA and ECDSA cryptographic key-pairs, creating Certificate Signing Requests (CSRs) from them, and combining the key-

pair with an issued digital certificate to create a secure portable container (PKCS12, JKS, JCEKS, etc.)

6. Libre Office, for signing documents including documents with signatures
7. Firefox
8. A program for signing video files. Candidates are mendelson OFTP2 , dsig , Opensignature , j4sign , and others from http://sourceforge.net/directory/os:linux/freshness:recently-updated/?q=digital+signature

The Tabelio Attestation Officer will meet additional qualifications.

See the Public Authority Component specifications for qualifications of an Attestation Officer.

VIVOS® lets the enrollment professional perform the following:

1. Verification of Identity

The identity of the candidate for enrollment is verified by means of expert examination of identity documents and, where available and legal, through a process of PII corroboration.

For lower enrollment quality scores, we will rely upon the skills of the Signing Agent. Attestation Officers will be trained to use UV light source, ID Checking Guide, and procedures that the INS makes available in the United States for verifying identity documents. Future machine verification of traditional credentials will use devices that use UV, infrared, and visible light reflection analysis, by machine reading of barcodes, and by machine analysis of typography and other graphic features.

Following document verification, the optional PII corroboration step takes place. Where PII corroboration service, also known as knowledge based authentication, is available and legal, VIVOS® connects to ChoicePoint AutoTrack XP, RSA Cyota, Riskwise InstantID, Equifax eIDverfier, RAF Sentinel, AMS Identicate, Accurint, or other KBA service, to provide corroboration of background information. The results are included in the Evidence of Identity files.

2. Capturing of Evidence of Identity Information

A copy of the Affidavit of Identity is kept as part of the Evidence of Identity submitted to the Osmio Vital Records Department, the certification authority. Other Evidence of Identity includes a still image of the identity document(s) taken by the Attestation Officer. Voice and facial image are captured in the video as the oath of identity is recited, and are part of the Evidence of Identity information. Tabelio Attestation Officers also capture fingerprint, iris, and hand vein information.

All Evidence of Identity is encrypted using the Osmio VRD Identity Evidence Encryption Public Key.

3. Administration of Oath

The candidate has filled in a secure Web form — an affidavit of identity — preferably before the appointment. The completed affidavit is printed by VIVOS® before or during the appointment and is then secured onto the VIVOS signature capture clipboard peripheral.

The affidavit is then read from the screen by the candidate while his or her right hand is raised.

After the oath is recited, the candidate signs the affidavit in the presence of the Attestation Officer. The Attestation Officer then signs the document, seals it with his or her notary seal, and stamps it with his or her notary commission stamp. In some jurisdictions the seal must then be inked.

4. Generation of Keys

The default for encryption type and key length is a 2048-bit RSA. The subject or principal relying party may alternatively request 1024-bit RSA or 4096-bit RSA keys. We should be prepared for requests for elliptic curve keys.

Foundational key pairs should not be generated in wallets (smart cards etc.) but rather should be generated on VIVOS or on the subject's own computer. Key pairs for chained certificates may be generated in wallets.

5. Submission of Certificate Signing Request

Using CSRtool or Charismathics Configurator, a Certificate Signing Request that includes Evidence of Identity information and the Foundational Public Key is generated.

6. Issuance of Digital Certificate and Osmio VRD Wallet(s).

Osmio VRD Wallets can take a number of forms.

- MicroSD Transceiver Chips (for phones)
- SIM Chips (for phones)
- Smart cards
- USB key fobs
- iButton jewelry
- Proximity and vicinity devices
- Others

Wallets must be of types that incorporate a processor, so that the private keys for the various key pairs, once embedded in the token, never need to leave the token.

The card writer writes cards that conform to Java Card Management Specifications Version 1.0b. Other card formats and standards may also be accommodated.

The Reliable Identities System calls for a wallet that supports multiple key pairs as well as a simple serial number. Such wallets ("tokens") are not yet widely available, but new designs are rapidly emerging.

7. Registration of Digital Birth Certificate

An event record is created using VIVOS's GPS location peripheral, signed traceroute record, USNO signed time stamp, video, biometrics, affidavit, and passport. The event is journaled using the National Notary Association's ENJOA™ automated notarial acts journaling system.

Files are digitally signed by both the Attestation Officer and the candidate, who is now considered a member.

VIVOS is equipped to transmit with its 802.11b wireless transceiver, or via its Ethernet NIC with RJ45 connector, or, where a wireless or wired network is not available, via its telephone modem. Files are transmitted using a 128-bit SSL session key after the equipment and its operator, the Attestation Officer, are properly authenticated.

Files are accessible only to the person who is authenticated and to any other properly authenticated individual or role occupant who is granted explicit permission through the Personal Information Ownership System of the owner of the files, which is the authenticated individual, or by law enforcement officials with a specific court order.

8. Offer of Escrow Services

In some cases subjects will benefit from having Evidence of Identity information available upon request by relying parties who have been licensed by the subject to have it, to prove that they are actually the ones who were enrolled with the public keys that were presented. Subjects also may wish to have the Attestation Officer keep a copy of their Foundational PENs to eliminate the risk of losing it. Escrow services will be explained and offered to the subject. If escrow services are declined, all files will be destroyed after the Foundational Certificate and PEN are successfully issued and tested.

When used to load tokens that have built-in fingerprint readers, the fingerprint for the token is captured separately.

Stepwise Enrollment Procedure

Following is a detailed description of the procedure for the issuance of an Osmio VRD Wallet by a Tabelio Officer using the VIVOS® Enrollment Workstation. The candidate for the credential is called an "affiant" (an affiant is one who signs an affidavit).

Before the appointment:

The subject will be directed by the principal relying party (employer or other entity paying for the enrollment) to go to a particular url. At the url, a welcome page will briefly explain the enrollment process, followed by a "Proceed with Enrollment" button.

Upon clicking the "Proceed with Enrollment" button, the subject will be presented with an https page. The page will note that at the end of the online enrollment preparation process an Affidavit of Identity will be produced, and will be sent to the subject's email address, followed by an email address input block. It also may be sent to a Notary Signing Agent's or Attestation Officer's email address, and will prompt for that address as well.

The form then will prompt for identity information from the subject's paper birth certificate and other information that will appear on the affidavit. Prompted items will include: name given at birth, names of parents, address(es) of parents, place of birth, date and time of birth, current legal name, nicknames, and aliases.

Completing the web form generates a pdf that includes the information inserted into the online form, resulting in the Affidavit of Identity pdf document. Before the meeting between the subject and the Attestation Officer or ASA (any signing agent) the subject will have completed the form and printed out the resulting affidavit document. At the discretion of the Attestation Officer, the filing of the web form may be done at time of appointment if necessary.

At appointment:

The affiant presents credentials to the Authentication Officer (Tabelio Officer or other ICCAP-Certified Authentication Professional) and, if not sponsored (by an employer, for example), pays the fee.

The Tabelio Officer explains the process and options, such as key escrow agency services.

If the credentials include a driver's license, the license is scanned through either its bar code reader or its mag stripe reader, depending upon which state/province and version of the license is presented.

ID is verified in offline mode first. If the license passes offline mode, and if the jurisdiction issuing the credential provides online verification, the verification is performed.

If the credentials include a passport, the passport is scanned by the passport verification system.

If the process takes place in North America, the U.K., Australia, or other places where PII corroboration is legal and a PII corroboration infrastructure is available, the authentication officer connects online to the designated PII corroboration service. Questions are presented and answered.

A fingerprint is read and recorded.

An iris is scanned and recorded.

A face photo is taken and recorded.

A driver's license is photographed and recorded.

A connection is made to Equifax, Experian, or Trans Union; identity information is compared and captured.

The time and location are stamped and signed from DeLorme GPS unit and USNO.

An affidavit is printed.

The Tabelio Officer goes over the affidavit:

"I hereby swear (or affirm) that

1. My full name is ___________________________. I was born on [date] in [place]. My full name, given to me at birth, is ______________________________________.

On [date] my name was changed to ______________________ [other changes – include all changes]

2. The difference between my name as specified on my driver's license and my legal name is [give differences. If there are differences between legal name and name on passport, specify those differences also].
3. I am also known by various people as [give nicknames, pen-names, aliases]
4. Address information
5. Social security number
6. [I hereby provide my resume as an exhibit of my working history.]
7. [Any other identification credentials are mentioned. Explain to affiant why credit card information should be included, in case there is ever an attempt at identity theft.]

Camera is turned on, affiant raises right hand and swears to information on affidavit; oath is recorded

RAO software is launched (if not already running)

A serial number is generated

Key pairs (two-factor and three-factor) are generated

Passphrase is entered three times via keyboard

All enrollment information is encrypted using affiant's public key

A hash of enrollment information is made and signed by the Tabelio Officer

Affiant grants the Tabelio Officer one-time permission to read all information to verify what is recorded

The Tabelio Officer records on Personprint™ that files are verified.

The affiant signs the affidavit on a signature pad clipboard

The Tabelio Officer notarizes the affidavit

The Tabelio Officer records the notarial act in a record book

A CD of the encrypted files is burned, placed in a jewel case, and given to affiant

The event is journaled using ENJOA™

The Tabelio Officer connects online via either modem or Ethernet to the Records Server

The system initiates a file transfer, deletes the files from VIVOS, logs off

The Tabelio Officer briefly reviews what has happened, instructs the authenticated individual about password protection and the use of the token, and gives the authenticated individual two instructional wallet cards

A hard token(s) is issued to the affiant

The session ends.

The swearing of an affidavit is not yet a paperless process and probably never should be. Following is the Affidavit of Identity used by the Tabelio Officer in enrolling a candidate with the use of the VIVOS® Enrollment Workstation. The form is preprinted with information from the Web session before the enrollment session, and is executed on a signature-capture clipboard that is connected to the VIVOS® Enrollment Workstation via a USB cable. The signatures become a part of the digital record of the event, just as the printed form, with wet signatures and notary seal, is a paper record of the event.

AFFIDAVIT OF IDENTITY

STATE OF________________________COUNTY OF _______________¬

I, [name] , being duly sworn, and under penalties of perjury, state that:

I reside at [address].

I was born on the date [birth date] at [birthplace].

The name given to me at my birth was [name].

The names of my parents at the time of my birth were [names of parents].

(optional) My address at the time of my birth was [address].

(If applicable) On [date] my name was changed to ______________________ [other changes – include all changes].

Add other identity information, as in the following examples:

The difference between my name as specified on my driver's license and my legal name is ______ .

I am also known by others as [nicknames, pen-names, aliases].

(optional) My [social security number] or [identify other government-issued identification number] is [number].

(optional) I hereby provide my resume or curriculum vitae as an exhibit of my working history.

[Mention any other identification credentials, including driver's license number if different from SSN.]

The biometric information that is obtained today by [Tabelio Officer's name] and that further identifies me is to be made part of this record.

I am responsible for determining under what circumstances the information in this record is to be disclosed, and to whom it will be disclosed, as specified in my Disclosure Practice Statement.

____ ______________

Signature Date

Jurat

Before me, a duly commissioned Notary Public within and for the State and County aforesaid, personally appeared ______________________ who, after being duly sworn as required by law, deposes and says the foregoing and that this affidavit is made for the purpose of establishing [his/her] identity for purposes to be determined by [himself/herself].

Subscribed and sworn to before me this ___ day of _______, 20__.

____

NOTARY PUBLIC

My commission expires _____________