Notarized Digital Signature

1 Problem Statement

The current PKI technology for digital signatures is able to provide the key needs for signatures viz. electronic authentication, proof of non-tamper and non-repudiation. The PKI digital signature technology, however, is not able to guarantee the identity of the owner of the PKI keys used in the signatures. It relies on a third party, such as Verisign, Thawte, Equifax etc., to have verified the identities of the users of the PKI based digital signature prior to issuing them a PKI key pair. Once the key has been issued, it is the responsibility of the key recipient to safe guard the key and inform the key issuer to revoke the key if the key has been compromised. Once the key has been issued, the key owner can use it for unlimited signatures with no involvement from the key issuer. This leaves a big hole in the security of the digital signatures and their legal validity. An offender may get access to user's key without his/her knowledge and use it to impersonate the user. The time lag between the time the key was actually compromised and when the user became aware of it could be substantial. This creates potentially big legal issues for both the signer and the consumer of the signed document such as financial institutions, governments and people at large.

Manoj Srivastava, founder and CEO of Infomosaic Corporation, has designed a system, which uses the public notaries to authenticate users during key issuance and for each electronic signature produced by using these keys. This idea was conceived on August 15, 2001. Manoj Srivastava has been working on XML digital signature tool development since June 20, 2001 and has been exploring various use cases for this technology. It is during this exploration, that he discovered the above problem and hence devised a solution. This idea was disclosed to Oleksandr V. Dron, an employee of Infomosaic Corporation, on August 16, 2001.

2 eNotarization System

The system consists of seven subsystems, which work together to provide the complete functionality:

1. Notary database management system
2. Notary enrollment and enrollment agent key management system
3. User key issuance and user key management system
4. Document signature and user database management system
5. Notary signature verification system
6. Payment and Billing system
7. Signed document signature verification system

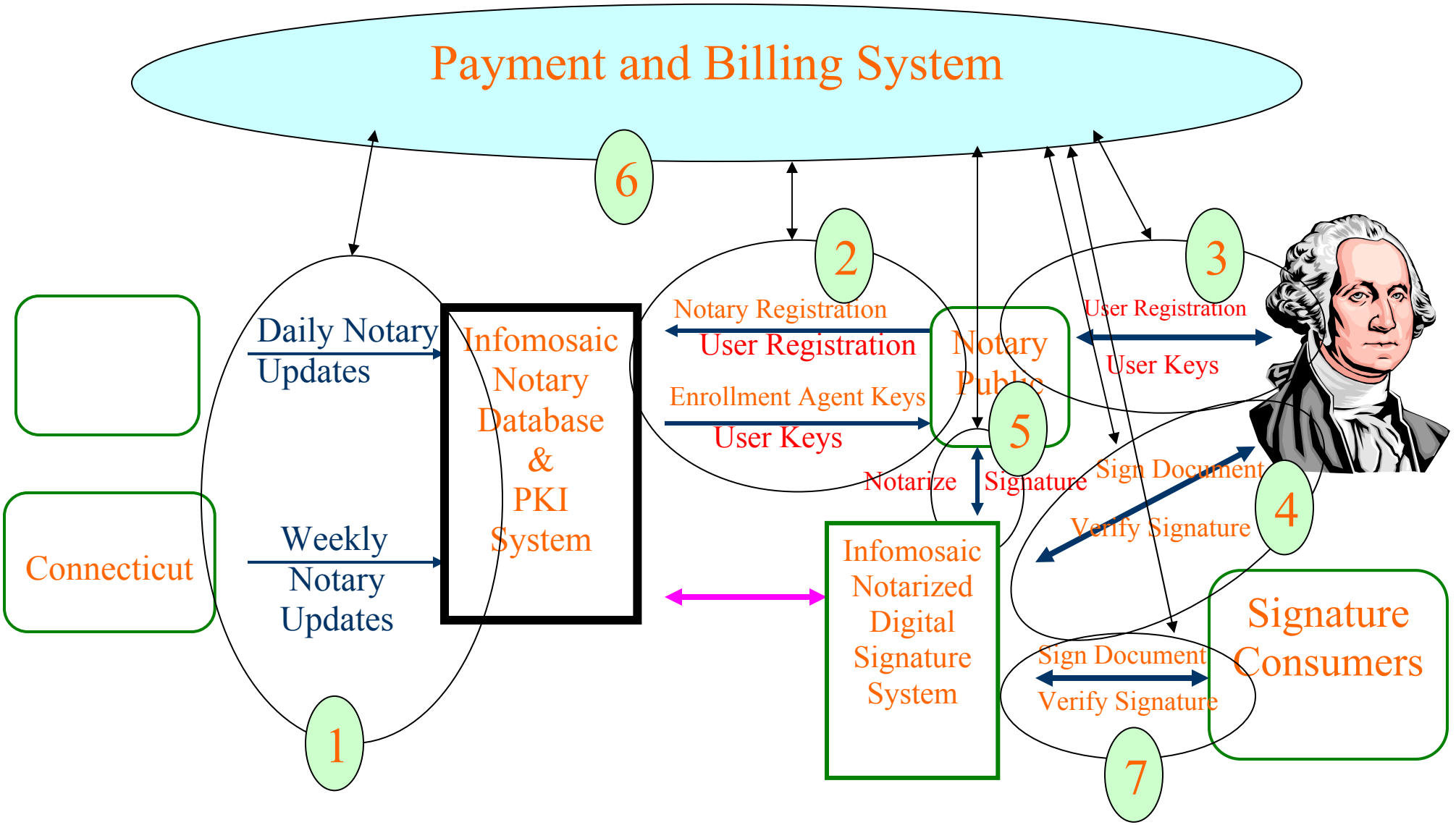
The notary public serves as an enrollment agent or an intermediate certificate authority. The notary database (1) is kept current with daily/weekly updates from the Secretary of State. Once a notary signs up as a digital notary using the notary enrollment system (2), s/he becomes an enrollment agent/intermediate certificate authority. Notary uses the User Key Issuance System (3) to issue keys to the general public after verifying their government issued identities as per various state regulations. The notary also scans and attaches a digital copy of this ID to the user database after encrypting it with his/her public key. This ensures that only the notary will be able to see the digital copy of this ID by decrypting it using his/her private key. If the notary chooses not to use the scanned images, s/he may simply enter detailed information of the ID such as ID type, number, expiration, issuing body, date of issue etc. and answers to some personal questions from the user, which the user can reproduce at a later time when signing any electronic document. These questions would be similar to the ones used by financial institutions, for establishing identities over the phone, such as, mother's maiden name, place of birth, favorite color, pet's name etc. This information is also encrypted using notary's public keys.

The user, once s/he has obtained a key from a notary, can use it to sign any electronic document digitally by using the Document Signature and User Key Management System (4). User logs onto this system to see a record of past activities and to create new signatures. During the signature process, user selects whether s/he would like to have the signature notarized. In the event s/he chooses notarized digital signature, s/he must present a digital copy of the ID, which was presented at the time to key issuance and/or answer all the personal questions, which were recorded during key issuance. Once this information is provided, the system produces signed document as per the XML digital signature standard. All personal information is kept on the server after encrypting it with the notary's public key and not attached to the signature. Once the notary has verified the personal information, the user can see and download a proof of notarization. If a normal signature (non-notarized) is chosen, no additional information is needed and the signature is produced as per the XML digital signature standard.

The notary logs onto the Notary Signature Verification System (5) where s/he receives request for notarization from all users who chose notarization and were issued key by this notary. The system automatically verifies the validity of the user key and presents to the notary, the encrypted ID and other personal information, which was recorded during the key issuance process. It also presents the encrypted ID and the personal information provided during the signature process. Both the set of information is decrypted on notary's computer using his/her private keys and s/he can verify their validity. Once s/he approves them, the system produces a record of notarization and records it in both the notary and user databases. Notary can download and print a history of all electronic notarization activity from this system for submitting to various state bodies. The system can optionally do this automatically, if the notary sets this option in his/her user profile.

The consumers of the signed documents log into the Signed Document Signature Verification System (7) to verify the validity of the notarization. If they don't need notary verification and authentication, they don't need to use this system.

All parties (user, notary and consumers) and system (the other 6 systems) work with the Payment and Billing System (6) to complete transactions. A fee is charged for key issuance, signing documents, notarization and notary verification.


Payment and Billing System
6
2
3
Daily Notary Updates
Weekly Notary Updates
Infomosaic Notary Database & PKI System
Connecticut
1
Notary Registration
User Registration
Enrollment Agent Keys
User Keys
Notary Public
5
Notarize
Signature
User Registration
User Keys
Sign Document
Verify Signature
4
Infomosaic Notarized Digital Signature System
Sign Document
Verify Signature
Signature Consumers
7