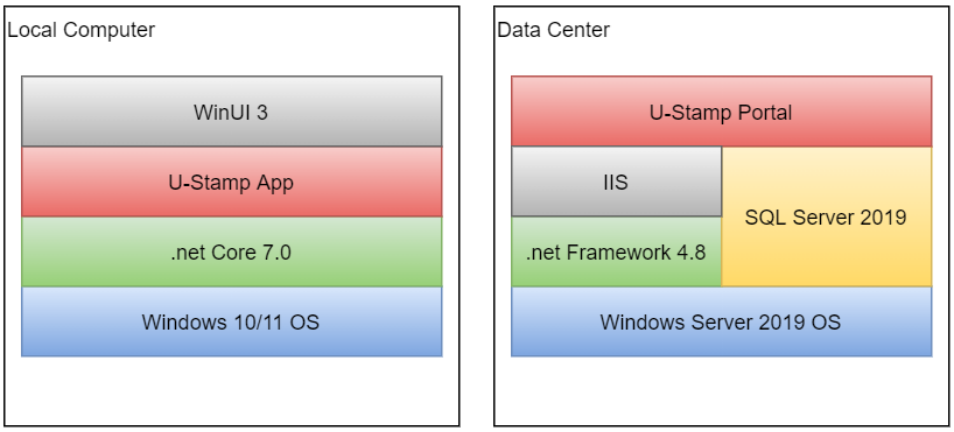
Taking the Electronic Medallion to the Next Security Level

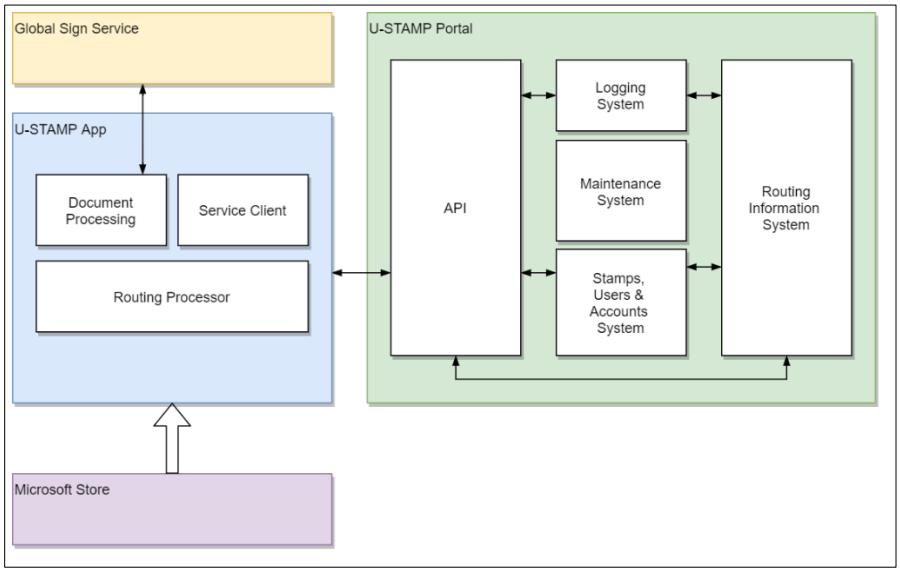
Abstract

Universal-STAMP ("U-STAMP") is the electronic platform for applying and verifying electronic Medallion Signature Guarantees. A pilot program has been active for more than a year as a portal where documents get stamped, transported, and verified. To meet increasing demands regarding the safeguarding of Personal Identifiable Information ("PII"), Hampton has upgraded the U-STAMP architecture to ensure neither Hampton nor Kemark receive any PII. This document gives an overview of the architecture and a description of the system components focusing on PII security.

Technology Stack



Architecture



Components

U-Stamp Portal

The portal serves as the central control mechanism for all transactions. Besides maintaining accounts, users, and stamps, transaction numbers will be generated, and logging (Audit Trail) is stored in a centralized repository.

- **API**
  Provides methods to securely access data within the portal. The API is used by the U-STAMP Application, however, will be exposed to customers for their own integration.
- **Routing information system**
  This subsystem holds the configuration for client's methods of secure communication for the routing processor (in the App)
- **Logging System**
  Creates and stores log entries about usage of the portal as well as document centric processing information (no contents, no PII)
  In addition, the document's hash value (SHA256) is stored with each transaction, so a document can be authenticated during the verification process.
- **Maintenance System**
  This is the web interface to the portal, and is used by Kemark to maintain accounts, additional users/stamps, etc.
- **Repository** (Stamps, Users, Accounts...)
  This is the system that stores accounts, users, and stamps.

Windows App

To limit all customer PII to the Guarantor institution that affixes the medallion on a document and to the firm receiving the transfer form, Hampton has created a U-STAMP Windows App. The app ensures all actions are under a Guarantor or Transfer Agent user's full control, adding and reviewing Medallion Signature Guaranteed documents without having to upload or send them to any server system unless intended. The App communicates with the portal using API calls via https, whereas these calls are authorized when the session starts (User/PW, TFA).

Once a stamp is applied, a digital signature is placed onto the PDF document using GlobalSign's external signature service. Thus, the signing certificate is not stored anywhere locally, and not on the portal either.

The App offers routing by e-Mail (i.e., open an Outlook E-Mail and attach the stamped document) in the first version.

- **Service Client**
  Connects to the portal's API and handles secure connections.
- **Document Processing**
  Loads, displays, and manipulates documents, adds digital signatures, and verifies documents.

Routing Processor

In a future version, routing documents from Guarantors to recipients of any kind (e.g., Transfer Agents) will be possible via methods other than email. The first option will be sftp whereby a Recipient decides to receive documents through its own sftp server.

Two Factor Authentication

U-Stamp will provide a Two Factor Authentication functionality to avoid password theft. Once a user logs in using username and password, a PIN is sent to his or her e-mail address. The PIN needs to be entered to complete the login. This also allows for using existing controls, since a log-in without access to corporate e-mail is not possible. (e.g. when offboarding employees)

External Security Services

Stafford

Hampton's third-party provider Stafford Associates (https://www.staffordnet.com/) is providing the service of hosting the database and the web based administrative app. The data center is certified for SOC 2 Type 2 and a summary of the report can be shared without NDA, the full report is available from Stafford Associates with the completion of an NDA.

Globa Sign

The GlobalSign Digital Signing Service allows for signing a PDF document without having to upload it, and without having to store a signing certificate locally. The method is called "External Signature." The process of applying a digital signature is split between client and server. The client generates the document's hash value and passes only that value to the GlobalSign Service. The service will encrypt this hash value using the signing certificate's private key, and return it to the client, which embeds it into the PDF document. GlobalSign also provides a certified time stamp, as well as LTV signing (so a verification can be performed years later.

Microsoft Store

The Windows App is available from the Microsoft Store, to serve as a trusted source for installations. All updates to the App will be handled through the Store. The app will be available in the store for free.
Access to the app will be provided through a private link from the program administrator Kemark Financial Services

For technical questions please contact:

Mario Kuttnig
mkuttnig@hamptontech.net
+1 (631) 9241335