# LESSON 7: FROM REQUIREMENTS TO SOLUTIONS

So far, this training has examined the CROMERR requirements in a couple of different ways. Lesson 5 presented the requirements as they are stated in the regulation. Lesson 6 examined the requirements by associating them with particular processes outlined in the CROMERR System Checklist.

Lesson 7 will provide another perspective on the requirements. It will provide examples of different approaches for meeting CROMERR requirements.

To help you choose solutions to comply with these requirements, Lesson 7 highlights:

- The relation between the CROMERR requirements and specific approaches to compliance; and
- Some key decisions in your compliance strategy that will affect your overall system design.

## FROM REQUIREMENTS TO SPECIFIC SOLUTIONS

**CROMERR REQUIREMENTS SET PERFORMANCE GOALS:**

- They specify the **WHAT** your system must be able to do.
- But, they do not specify **HOW** your system does what it does—except, to a very limited extent, for the identity-proofing requirements in the case of Priority Reports.

**CROMERR REQUIREMENTS DO NOT DICTATE SPECIFIC APPROACHES TO:**

- System functions;
- Operating procedures;
- System architecture; and
- Technologies used.

While currently available technologies may limit the choice of solutions for some of CROMERR's requirements, the requirements are written to allow the range of choices to expand as new technologies and products emerge.

## FROM REQUIREMENTS TO SPECIFIC SOLUTIONS

The task is to decide on particular solutions to meet the general performance goals.

**Consider these two examples**:

1. **CROMERR Requirement:** Provide an opportunity to review COR in a human-readable format.

- Requirement allows:
  - Delivery on paper, on magnetic or optical media, or electronically;
  - Delivery via online session, offline electronic transfer, or freight or postal carrier; and
  - Creation from data in a database or a copy of what was submitted.

- Solution could involve:
  - Printing to paper or disks;
  - Client-server transactions, file-transfer or email, or the U.S. Postal Service; and
  - XML or XSL formatting, PDF file capture, or other report generation functionality.

2. **CROMERR Requirement:** Issue (or register) a signing credential in a way that minimizes risk of compromise.

- Requirement allows:
  - Creation of credential by registrant, system, or third party; and
  - Credentials based on shared secrets (PINs or passwords), encrypted objects, biometrics, or physical tokens.

- Requirement could involve:
  - Cryptography, biometric readers, security of "secure socket layer" sessions, or the security provided by paper envelopes; and
  - Password- or PIN-generation functionality, enforcement of strength requirements for user-generated credentials, issuance and maintenance of user hardware, or interface with third party credential services.

## From Requirements to Specific Solutions—Two Key Decisions

As you consider particular solutions to meet the general performance goals, two decisions are especially important because of their broader implications for your system.

These key decisions are:

1. Type of credential used; and
2. What the system defines as the COR.

Consider these key decisions before establishing system specifications and design. The following pages discuss these key decisions and describe their impacts on overall system design.

As you think about different approaches, remember the implications and trade-offs associated with each decision.

### KEY DECISION 1: TYPE OF CREDENTIAL USED

Type of credential used determines:

- How Credentials are Issued—
  - Most credentials issued by or registered with the system require protection as they travel between registrant and system.
  - Credentials that are registered (rather than issued) may need the system to enforce strength requirements and—where issued by a third party—ensure authenticity.
  - Credentials that incorporate biometrics or include cryptographic keys will need specialized technologies to support them.
  - Credentials issued in connection with hardware tokens will require support for users' implementation.
- Approach to Binding Signatures to Document Content—
  - Credentials that include cryptographic keys may execute signatures that are automatically bound to the document being signed by incorporating a message digest or hash value uniquely related to the document content.
  - Other kinds of credentials lack this functionality, and so require an independent approach to signature binding.
- How Signatures are Validated—
  - Signatures executed with third party credentials require interaction with the issuing authority to determine that the credentials are authentic.
  - Credentials that provide cryptographic keys may require decryption functionality for validation of the signatures they execute.
- How Signatures are Included in the COR—
  - Credentials that are included "in the clear" in the signatures they execute (for example, as a PIN or password) need to be "shielded" in some way on the copies of record (COR), for example, by being encrypted or hashed.

**Hash Value—**Cryptographic hash functions are one-way mathematical algorithms that take an arbitrary length input and produce a fixed-length output string. The output is the hash value. A hash value is a unique and extremely compact numerical representation of a piece of data. It is computationally improbable to find two distinct inputs that hash to the same value (or "collide'').

For example, consider the following two types of credentials:

- Shared secrets in the form of PINs or passwords; and

- Certificates associated with private–public key pairs that are used to execute digital signatures.

| **Example Solutions** ▸ | **Solution A**<br><br>**PINs or Passwords** | **Solution B**<br><br>**Private–Public Key Pairs** |
|---|---|---|
| **Issuing Credential** | Requires Secure Socket Layer (SSL), Transport Layer Security (TLS) or another technology during setup to protect them as they travel between registrant and system. | The private key—which is used to execute the signatures—can be generated at the user's work station, so may not need to travel between registrant and system. |
| **Binding Signature to Document Content** | Execution of a PIN- or password-based signature does not bind it to the document signed, so the system must provide additional functionality to provide for signature binding. | The digital signature executed with the private key is bound to the document signed because the signature is just the hash value of the document content encrypted with the private key. |
| **Signature Validation** | Can rely wholly on internal system records of PINs or passwords registered or issued by the system. | Where the certificate associated with the key pair is issued by a third party—for example, where this is a PKI certificate—then validation requires interaction with the issuing authority to determine that the certificate is valid. |
| **Including Signatures in Copies of Record** | Signatures consisting of the PIN or password "in the clear" need "shielding" on the CORs—for example by being encrypted or hashed—so that PINs and passwords are not compromised by providing access to the CORs. | Access to a digital signature on a COR does not raise any issues of credential compromise because a digital signature does not include—and provides no way to derive—the private key needed to execute it. |

**Private–Public Key Pairs—**Each user has a pair of cryptographic keys—a public key and a private key. The private key is kept secret, while the public key may be widely distributed.

**Digital Signatures—**A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped.

**Public Key Infrastructure (PKI)—**PKI enables users of a basically unsecure public network, such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.

### KEY DECISION 2: DEFINING THE COPY OF RECORD (COR)

What the system defines as the COR determines:

- How the COR is Shown to be "True and Correct"—
  - The closer the COR is to the file received, the easier a "true and correct" showing may be, since there will be few or no transformations of that file to account for.
  - For CORs that do not have an associated hash value, a "true and correct" showing will depend heavily on how their access is secured, controlled, and logged.
  - If CORs can incorporate changes to their content—for example, to accommodate submitter corrections—then a "true and correct" showing will depend heavily on a chain of custody that documents all such changes and their circumstances.
- How the Opportunity to Review is Provided—
  - The COR's format will determine what processing is needed for a "human-readable" version.
  - The medium in which the COR is maintained (e.g. electronic or paper) will affect how it can be provided for review.

For example, consider the following ways a system can define the COR:

- A PDF capture of the on-screen appearance of the file submitted, associated with the signature, the date and time of submission, and a hash value of the file submitted
- The submitted data as stored in a database, associated with the signature and the date and time of submission.
- A print-out of the submitted data, including the signature and the date and time of submission.

| Example Solutions: ▸ | **Solution A**<br><br>**PDF Capture of the Submitted File** | **Solution B**<br><br>**Data in a Database** | **Solution C**<br><br>**A Paper Print-Out** |
|---|---|---|---|
| **Opportunity to Review the COR** | Requires making the PDF available online or sending it to the signer or submitter—as an email attachment or by other means—assuming the PDF captures a human-readable format. | Requires: (1) system functions to put the data into a human-readable format; and (2) making the formatted data available online or sending it to the signer or submitter by other means, such as an email attachment. | Requires procedures to: (1) receive requests; (2) produce paper copies; and (3) deliver the copies. |
| **COR is Shown to be "True and Correct"** | Requires a demonstration of the integrity of the PDF file, for example, by showing that it has been secured against tampering or that a hash value calculated from the file matches the hash calculated when it was received. | Requires a demonstration that: (1) the processing that placed the data in the database did not, in any way, affect its informational content; and (2) that the database has been secured against tampering and any undocumented changes. | Requires procedures to: (1) produce an accurate print-out of the submittal; (2) certify the print-out's accuracy; and (3) secure the print-out against any tampering or destruction. |

## From Key Decisions to CROMERR-Compliant Solutions

To recap, two key decisions addressed in this lesson include:

- Decision 1—the type of credential you use; and
- Decision 2—how you define the COR.

These will determine the available solutions for many, if not most, of the CROMERR System Checklist items that express the CROMERR requirements for your systems.

In the next, and final, lesson, we will focus on four critical checklist items that have an especially close connection with these two key decisions.