



HL7[®] FHIR[®] Security

Education Event

What's In Your ~~Web~~ Trust Store?
“Think popular banking commercial!”

About Me



- Over 29 years in the design, architecture, and implementation of Healthcare IT solutions; with intense emphasis, in recent years, on information security & privacy for various Healthcare solutions used in the marketplace
- Engineer at heart - and passionate about information security & privacy
- Serving as co-lead on the FHIR at Scale Taskforce (FAST – *now an HL7 Accelerator) Security Team

Disclaimers

- Tools used in this presentation are intended to demonstrate concepts and in no way constitute an endorsement of any kind
- The techniques shared today are for *use only in environments (e.g., development/test) where developers have permissions and authorization*

Wallet & Trust Store - huh😊?



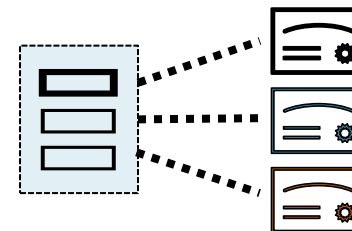
- It's an analogy of shared objectives between your wallet and trust store
- For example, a typical consumer wallet only *contains items from trusted sources*, particularly those you rely upon for secure financial transactions

Common Objectives

Consumer's Wallet



Trust Stores



You ensure...

- The contents are well-maintained
- To respond instantly to compromise or loss
- To never lose sight or not know how it's protected

As a developer
you ensure... ✓

Learning Objectives

- What a trust store is
- Their critical role in trustworthy, secure exchange
- Learn about example FHIR exchange scenarios where they apply
- Best practices...
 - Trust store management
 - Where they are located
 - Developer tools & tips to diagnose errors



What is a trust store?

- A file¹ containing a collection of X509 digital certificates of certificate authorities (CAs) considered trusted by an application or system
- Digital certificate⁸ (X509) is a document that proves the identity and authenticity of a person, organization, or service on the Internet



X509

These digital certificates are the foundation of Public Key Infrastructure² (PKI)

What is a Certificate Authority (CA)

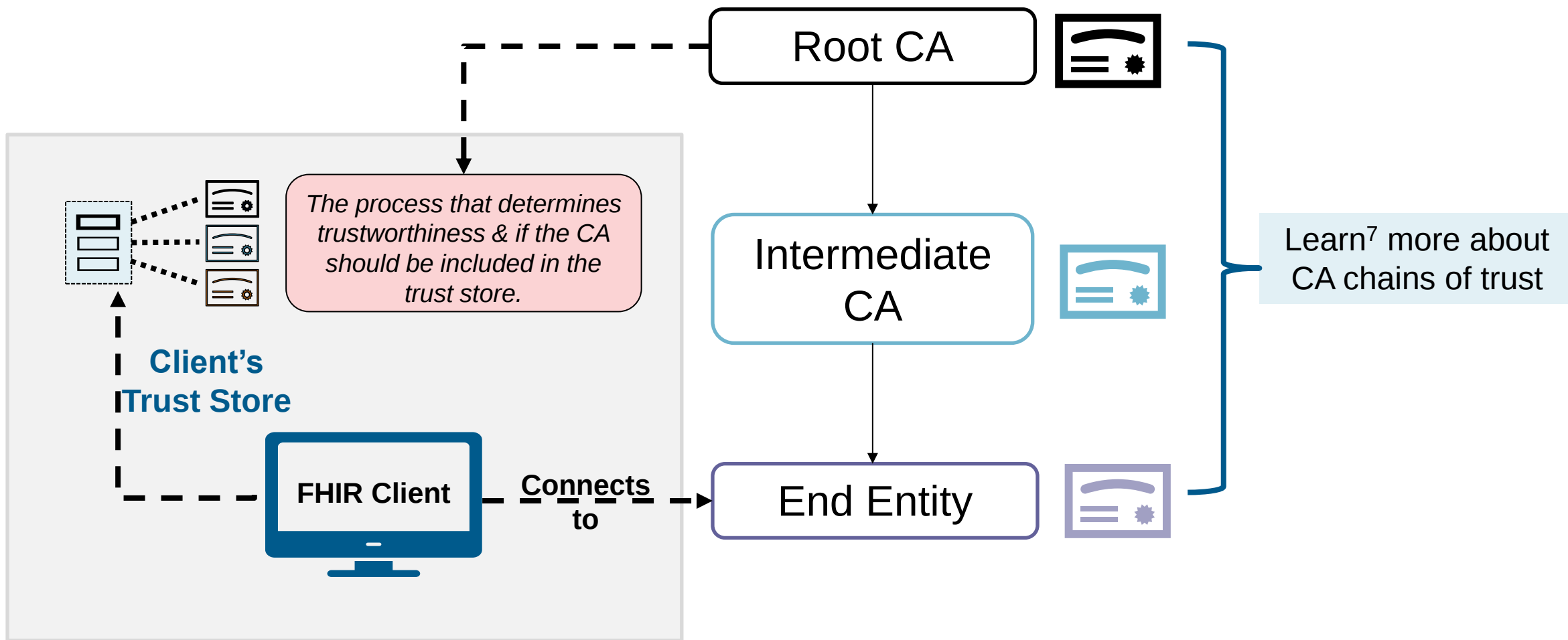
- A [certificate authority \(CA\)](#) is a trusted organization that issues digital certificates for websites and other entities
- Without CAs, shopping, banking, any exchange of sensitive data, or browsing online would be less secure
- Recognized audits ([example](#)) are critical to ensure CA operates and complies with requirements

Their Critical Role

- Helps ensure secure connections with trusted third parties, such as web servers, APIs, or cloud services
- Referenced in a verification³ process that ensures certificates presented by third parties were issued by a trusted certificate authority (CA)
- *Robust Implementations* safeguard against potential impersonation or tampering by malicious actors.



CA Chain



CA Analogy

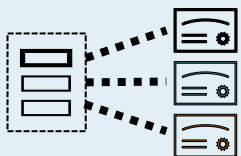
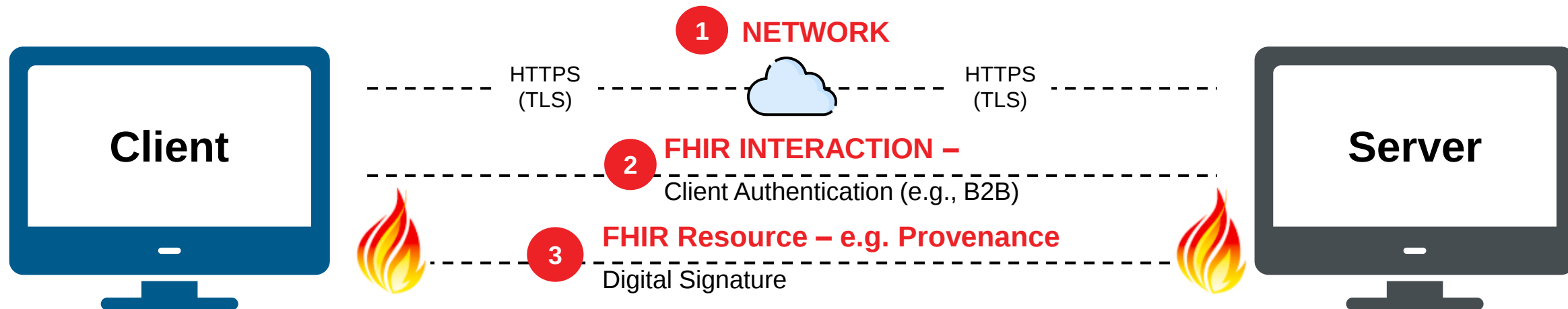
- At what lengths would a professional skydiver go...
 - to ensure the provider of their parachute is trustworthy?
 - to ensure they had proper safety training?



X509

Before you include a CA in your trust store, what will you do to ensure its trustworthiness & best practices are applied during its lifetime?

Understanding trust in the context of FHIR



IMPORTANT: Each context may involve a distinct trust store

Example Context / Scenarios

Example Context / Scenario	FHIR Reference
1 NETWORK / Secure communication between a client and server over a network.	<i>Communications</i> - https://hl7.org/fhir/security.html#http
2 FHIR INTERACTION / • B2B Client authentication to a Token Endpoint • SMART Asymmetric (“private key JWT”) authentication (confidential clients)	<i>UDAP JWT-Based Client Authentication</i> - https://hl7.org/fhir/us/udap-security/b2b.html#submitting-a-token-request <i>SMART App Launch</i> – https://hl7.org/fhir/smart-app-launch/#asymmetric-private-key-jwt-authentication
3 FHIR RESOURCE / Digital Signature Validation – such as a Provenance Resource	<i>Digital Signatures</i> - https://hl7.org/fhir/signatures.html#6.1.2

BEST PRACTICES⁴

How they are managed⁴

- Should only include certificates for trusted CAs necessary for the specific context and scenario
- Perform routine maintenance to remove expired or revoked certificates and add new or updated ones
- Ensure trust stores are monitored continuously for tampering & alerting when necessary
- Should be stored securely per organizational policies & standards (e.g., encryption/password protection)

- ***Contents are well-maintained***
- To respond instantly to compromise or loss
- Never lose sight or not know how it's protected

Respond instantly to compromise or loss

- Recovery
 - Test plans that account for trust store integrity, loss, or misconfiguration
- Ensure your implementations account for & test applicable best practices for...
 - Certificate Revocation Lists (CRLs) - blacklist
 - Online Certificate Status Protocol (OCSP)
 - Certificate Transparency Logs⁶
Who watches the watchers?

- Contents are well-maintained
- **To respond instantly to compromise or loss**
- Never lose sight or not know how it's protected

Typical Locations

- Depends on the operating system, runtime environment, or tool
- Such as...
 - **Linux**: /etc/ssl/certs or /usr/share/ca-certificates
 - **.NET**: Windows Certificate Store (accessible through the certmgr. msc tool or the X509Store class)
 - **Java**: \$JAVA_HOME/lib/security/cacerts or \$JAVA_HOME/jre/lib/security/cacerts
 - **Python**: The system's certificate store or a custom file specified by REQUESTS_CA_BUNDLE or CURL_CA_BUNDLE environment variables
 - **OpenSSL**: specified by SSL_CERT_FILE or SSL_CERT_DIR environment variables
 - **curl**: /etc/ssl/certs or /etc/pki/tls/certs

- Contents are well-maintained
- To respond instantly to compromise or loss
- **Never lose sight or not know how it's protected**

***TIP:** Become familiar with the different formats ([refer to the appendix](#))*

DEMONSTRATION

Demos

- NETWORK (e.g., https)
- FHIR INTERACTION
- FHIR Resource

TIP: Take time after this session to learn about FHIR Digital Signatures⁵ as expressed by John Moehrke.



THANK YOU!

References

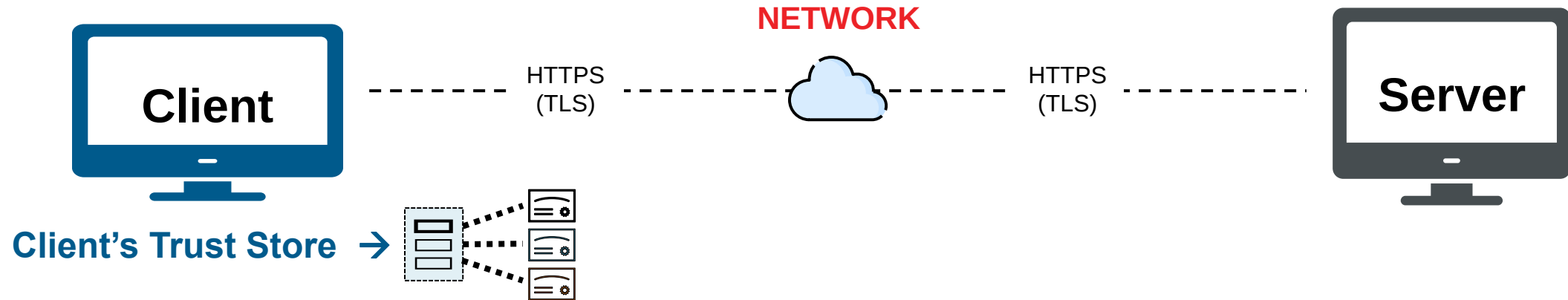
1. File or repository
2. <https://tools.ietf.org/html/rfc5280> (PKIX Certificate and CRL Profile)
3. https://en.wikipedia.org/wiki/Certification_path_validation_algorithm
4. <https://sslinsights.com/what-is-trust-store-and-how-to-manage-it/>
5. <https://healthcaresecprivacy.blogspot.com/2024/08/fhir-digital-signatures.html>
6. <https://certificate.transparency.dev/>
7. https://en.wikipedia.org/wiki/Root_certificate
8. <https://www.portnox.com/cybersecurity-101/x509-certificate/>

APPENDIX

Trust Store Formats

Format	Extension	Description
PEM (Privacy-Enhanced Mail)	.pem	A text-based format that uses Base64 encoding and delimiters such as "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----"
DER (Distinguished Encoding Rules)	.der	A binary format that encodes the certificate as an ASN.1 structure
PKCS#7 (Public Key Cryptography Standards #7)	.p7b	A binary format that can store multiple certificates in a single file, optionally with a signature
PKCS#12 (Public Key Cryptography Standards #12)	.p12 or .pfx	A binary format that can store one or more certificates along with their private keys, protected by a password
JKS (Java Key Store)	.jks → .p12	A proprietary format used by *Java applications that can store multiple certificates and private keys, protected by a password <i>*Recent Java versions default to the PKCS12 format</i>

Demo - Network



Tool: OpenSSL

trust-store-a-context.pem

trust-store-b-context.pem

Includes this CA

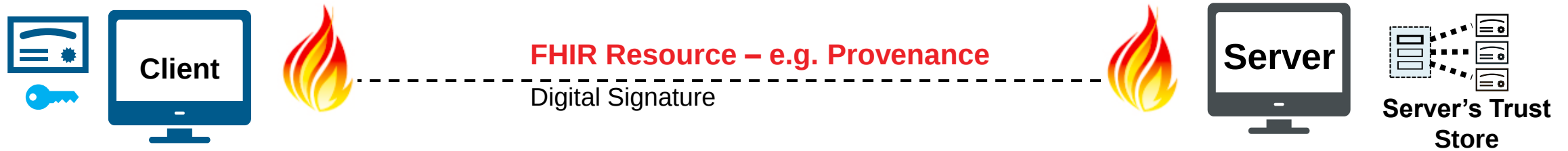
Includes this CA

See HL7 – Public Test Servers

[ISRG Root X1] hapi.fhir.org

[Amazon Root CA 1] demo.kodjin.com

Demo – Digital Signature



- Such as a FHIR Resource with an associated [digital signature](#)
- Example <https://hl7.org/fhir/provenance.html>

patient	TU	0..1	Reference(Patient)
encounter	TU	0..1	Reference(Encounter)
agent	Σ C	1..*	BackboneElement
entity	Σ TU	0..*	BackboneElement
signature	TU	0..*	Signature



- Signature Data Type
 - <https://hl7.org/fhir/datatypes.html#signature>
- Helpful References
 - [JSON Signature Rules](#)
 - [XML Signature Rules](#)



FHIR Client Private Key (protected!)

DEMO – FHIR Interaction



Private Key JWT – Client Authentication

- IG - [Security for Scalable Registration, Authentication, and Authorization](#)
- [Creating Authentication Token](#)
- [Example of library use](#) (Java → [Nimbus](#))

Server Side – Token, Signature & CA validation

- Per IG – [Validate Token; including CA validation for trustworthiness](#)

TIP: Take time after this session to learn about FHIR Digital Signatures⁵ as expressed by John Moehrke.

Tools & Tips

■ Tips to warm-up

- Given the nature of the FHIR interaction, what trust store is used?
- Where is it located & what access permissions are in force
- Know the trust store format ([see slide 23](#))
- Use well-tested libraries to do the validation (*never roll your own!*)
- Use tools to list the contents of the trust store
- Use tools to manually validate X509 certificate against a given trust store

■ Tools

- openssl (such as verify certificate using a given trust store, output x509 certificates as text, covert formats, etc.)
- [Java Keytool](#) (such as importing CA X509 into the *appropriate trust store*)

