X9 Financial PKI Frequently Asked Questions

1. What is the X9 Financial PKI, and why is it important for financial institutions?

The X9 Financial public key infrastructure (PKI) is an industry-governed public key infrastructure framework designed specifically for the financial services sector. It is governed by **ASC X9** and provides a dedicated trust root intended for non-browser use cases such as:

- System-to-system communication
- Mutual TLS (mTLS)
- Secure APIs

2. Why is DTCC making this change?

DTCC is making this change **in response to industry-wide updates to TLS certificate governance issued by the CA/Browser Forum**, which applies to all organizations using public CA certificates.

Key changes driving this transition include:

- **Removal of Client Authentication (ClientAuth EKU)** from public CA certificates, making them unsuitable for use cases such as mutual TLS (mTLS) and system-to-system integrations
- **Progressive reduction in certificate validity periods,** significantly increasing operational complexity and reducing long-term stability

As a result, public CA certificates will no longer reliably support non-browser, machine-to-machine communication scenarios used by DTCC clients.

To address these industry changes, DTCC is adopting X9 Financial PKI, which:

- Supports continued use of mutual TLS (mTLS) for secure machine-to-machine connectivity across DTCC services.
- Reduces DTCC's exposure to changes in public CA policies that are increasingly focused on browser-based use cases.
- Provides a certificate framework designed for financial services system connectivity.
- Helps minimize future client and operational impacts arising from shortened public certificate validity periods.

3. What impact will the X9 PKI have on financial cybersecurity?

By providing a dedicated, scalable, and secure PKI infrastructure, the X9 PKI helps financial institutions:

- **Reduce cyber security risks** by eliminating reliance on external browser-based certificate policies
- **Ensure long-term stability** with a trusted industry-backed root certificate
- **Enhance compliance** with evolving financial security regulations

4. What actions are required from DTCC Clients?

To ensure continued connectivity and prevent service disruption, Clients **must** complete the following actions:

- **Add the X9 Financial PKI root and required intermediate certificates to applicable trust stores**. Clients can do this anytime, as this will not change their systems' behavior until an X9 certificate is presented during a connection establishment.
- Verify that **all relevant systems trust the X9 certificate chain** (e.g., application servers, APIs, gateways, load balancers or internet edge providers, such as Akamai or Cloudflare).
- Review, update and test any certificate custom validation logic, if applicable. Remember that **DTCC does not support Certificate Pinning.**
- As required, Client must set up their systems to **present X9 certificates** during mTLS connection establishment, which includes purchasing X9 certificates and installing them in the prescribed timeframes.
- When requesting X9 certificates from DigiCert for DTCC connectivity, Clients using TLS 1.2 or earlier should ensure the certificate is issued with the Key Usage attributes "**Digital Signature**" and "**Key Encipherment**". DigiCert's X9 certificate request process defaults to "**Digital Signature**" only unless otherwise configured. Failure to include Key Encipherment may result in compatibility or TLS connectivity issues and could require certificate reissuance.
- Clients may also configure DigiCert CertCentral to default X9 certificate requests to "Digital Signature and Key Encipherment" to ensure consistent certificate issuance for TLS 1.2 and earlier environments
- Implement all X9-related changes in a single coordinated activity by the specified important dates. Implementing changes incrementally may result in mismatched configurations and increase the likelihood of service impact.

5. What protocols are impacted?

X9 Financial PKI Certificate – Impacted Protocols

The following connectivity protocols are impacted. Please do not make X9 changes to any other connectivity protocols unless further instructed:

Protocol	Action
MQ	Clients must **trust** and **present X9 certificates** (mTLS) **for both inbound** connections to DTCC and **outbound** connections from DTCC
Connect: Direct (NDM)	Clients must **trust X9 certificates** for **inbound** connections to DTCC
FTPS	Clients must **trust X9 certificates for inbound** connections to DTCC
Insurance REST and SOAP API's	Clients must **trust** X9 for **outbound** connections from DTCC. Inbound connections to DTCC are not impacted

6. Required Client Readiness Dates

Connectivity / Protocols	Test environment	Production environment	Readiness requirement

MQ, NDM, FTPS	By November 30, 2026	By December 31, 2026	Clients must complete these activities for MQ, NDM, and FTPS by the specified dates to avoid connectivity disruptions when DTCC begins renewing certificates in Q1 2027.
Insurance REST and SOAP API's	By February 28, 2027	By March 31, 2027	Clients must complete these activities for Insurance REST and SOAP APIs by the specified dates to avoid connectivity disruptions when DTCC begins renewing certificates in Q2 2027.

7. Where can Clients download the X9 PKI root certificates?

The root certificates for the X9 PKI are available in the DigiCert Knowledge Base. Clients must install and trust the full **DigiCert X9 Financial PKI RSA-4096 certificate chain** used by DTCC.

This consists of **one root certificate and two intermediate certificates**:

X9 Financial PKI - RSA 4096 Root Download PEM | Download DER/CRT

X9 Financial PKI – RSA 4096 ICA Download PEM | Download DER/CRT

X9 Financial PKI – RSA 4096 ICA EU Download PEM | Download DER/CRT

Please ensure that you are downloading the latest root and two intermediate certificates from DigiCert.com, the above embedded links are as of June 30, 2026.

8. How do Clients identify whether the certificate is Web PKI or X9 PKI, and what certificate type to be used?

Web browsers operate on standards set by the CA/B Forum, and other industry compliance protocols designed specifically for the internet. X9 PKI operates on standards and compliance that meet the needs of finance.

Unlike the traditional web PKI, which was built to serve browser needs, the X9 PKI provides independent, stable, and secure digital certificate management.

Please refer to the comparison table in the Appendix below for more details, and which certificate identification and type to be used.

9. What happens if Clients do not update their trust stores with X9?

Failure to update trust stores will result in TLS handshake failures, leading to potential **service disruption** and **loss of connectivity** for certificate-based integrations.

10. Does this impact browser-based user access?

No. This change applies only to **system-to-system connectivity (both TLS and mTLS)** and not to browser-based access. Web browsers operate on governance standards set by the CA/B Forum X9 PKI based on governance standards and compliance that meet the needs of the finance ecosystem.

11. Will DTCC provide X9 certificates?

No. If clients need to install Root and Intermediate certificates in their trust stores, the certificates can be downloaded freely from the DigiCert website details are provided below.

If clients need X9 end-entity certificates to present to DTCC for authentication during connection establishment, then they must purchase these certificates from DigiCert, the only organization authorized at the present to issue such certificates. Details are provided below.

12. Will there be a transition or coexistence period?

The current transition period allows clients to begin adopting and trusting X9 certificates early. DTCC will not present an X9 certificate until Q1 2027 as existing certificates expire and get updated to X9 as part of the lifecycle maintenance. Clients must complete their readiness activities before the published timelines to ensure uninterrupted connectivity.

For mTLS connections, DTCC needs to present a certificate to the client, and the client needs to present a certificate to DTCC. DTCC will not present an X9 certificate until Q1 2027 as existing certificates expire and get updated to X9 as part of the lifecycle maintenance

For client-initiated connections to DTCC, X9 Financial support is available today.

13. What should clients do if they share a queue manager with multiple vendors that may not all be ready to present X9 certificates?

Clients should keep their existing queue manager personal (leaf/end-entity) certificate in place for vendor channels and configure the DTCC channel's CERTLABL to present the new X9-signed personal certificate This allows the DTCC X9 migration to proceed without requiring all vendors that share the queue manager to adopt X9 certificates at the same time.

14. Who should Clients contact for support?

Clients should contact TechnicalChangeEnablement@DTCC.com for queries

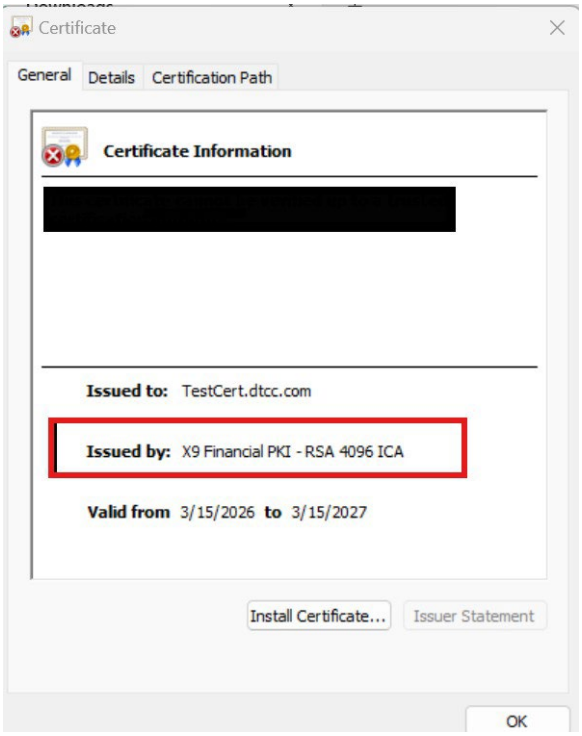
This FAQ is provided for informational purposes only and should be read in conjunction with official DTCC client communications.

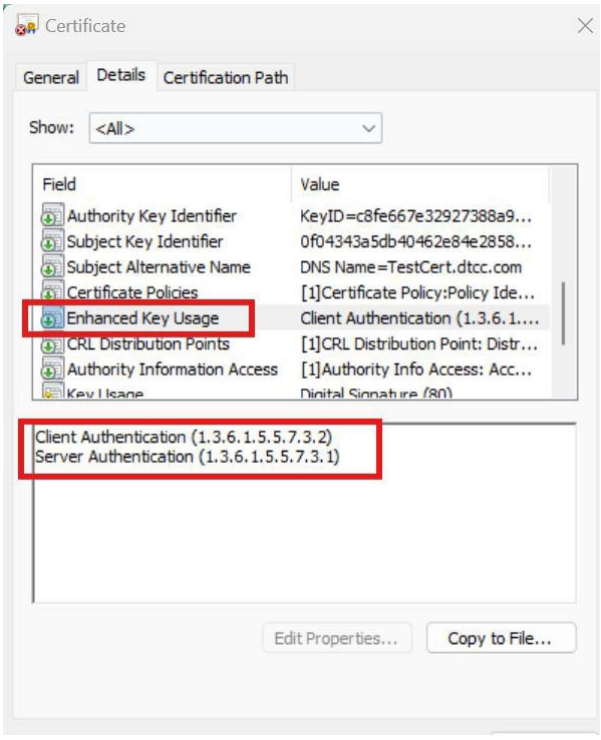
Appendix

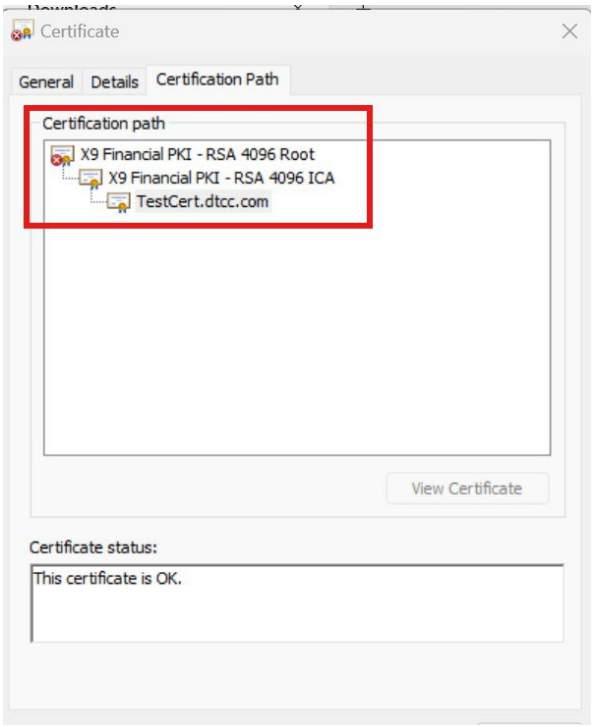
Web PKI vs X9 PKI – Quick Comparison

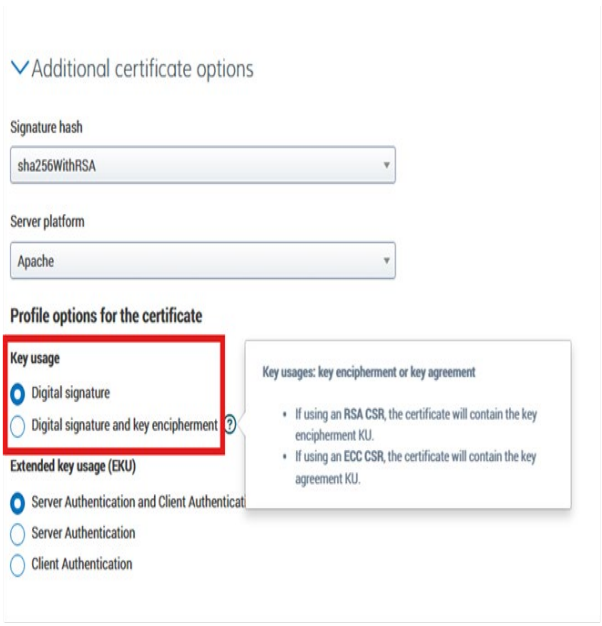
Category	Web PKI	X9 PKI (Financial PKI)
Primary Purpose	Secure websites and browser traffic (HTTPS)	Secure system-to-system communication (APIs, MQ, file transfer, mTLS)
Trust Model	Public trust (auto trusted by browsers/OS)	Private trust (controlled by financial ecosystem)
Root / Trust Anchor	Pre-installed in browsers and OS	Must be installed in enterprise trust stores
Certificate Issuers	Public Certificate Authorities (e.g., DigiCert, SSL.com, Sectigo)	Financial PKI Certificate Authorities (Currently, only DigiCert X9)
Certificate Chain	Public Root -> Intermediate -> Server Cert	X9 Root -> Intermediate -> Client/Server Cert
Client Authentication (mTLS)	Not supported going forward	Fully supported
Extended Key Usage (EKU)	Server Authentication only	Client Authentication and/or Server Authentication (Dual EKU supported)
Typical Use Cases	Websites, portals, browser APIs	MQ, NDM, FTPS, APIs, backend systems
Trust Behavior	Works automatically	Requires trust store update
Lifecycle	Short-lived, frequent renewal as mandated by the CA/B Forum	Longer, policy-driven
Governance	CA/Browser Forum	ANSI X9 financial standards
How to Identify	• Issued by: Public CA (e.g., DigiCert) • EKU: Server Authentication only	• Issued by: X9 Financial PKI EKU: Client Authentication and Server Authentication

Screenshots of an Example X9 Certificate









Doc Date: October 7, 2026
Publication Code: CP_2036
Service: Cross-Product
Title: X9 Financial PKI Frequently Asked Questions