General Services Administration (GSA)

Access Certificates for Electronic Services (ACES)

Transition FAQ Sheet

v1

December 20, 2017

Background

The GSA General Counsel recommended to the GSA Access Certificates for Electronic Services (ACES) Program Management Office (PMO) the ACES program be sunset. There are three reasons cited by the General Counsel:

1) The General Services Administration primary mission is deliver the best value in real estate, acquisitions, and technology services to the government. Operating a citizen-based PKI, such as GSA ACES, is outside the scope of GSA's mission.
2) GSA vendor programs need at least three commercial vendors to establish a competitive need. The ACES program only has two vendors which was reduced to one in August 2017.
3) The Federal PKI has matured since the establishment of ACES and offers a variety of PKI services for business partners and citizens.

The ACES Program Manager has acted on the General Counsel recommendation and will implement a sunset plan which includes a two-year transition for ACES vendors and relying parties.

Tentative Transition Timeline

The sunset plan implementation will be in three phases.

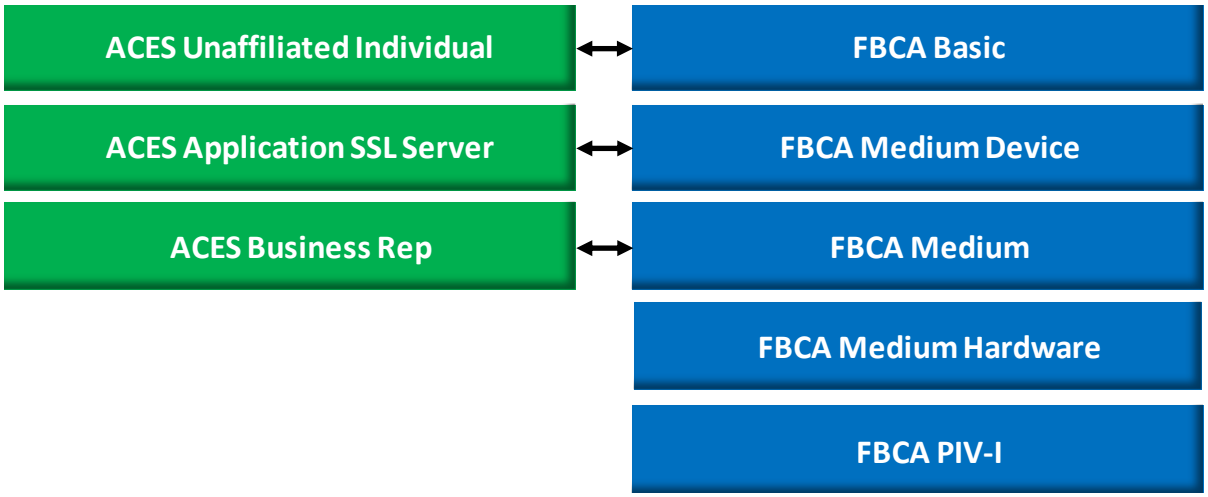
A. Phase 1 – Inform (FY18Q1 – Q2)
    a. Notify ACES vendors and federal relying parties of the sunset recommendation and transition plan.
    b. After understanding vendor and federal relying party impact and needs, develop transition guidance and a public sunset announcement.
    c. In January, release the public announcement after ACES vendor and federal relying party meetings.
B. Phase 2 – Transition (FY18Q2 – Q3)
    a. The ACES PMO will collaborate with the ACES vendors and federal relying parties to transition to Federal PKI alternatives that are comparable to ACES certificates.
    b. The federal relying parties will be instructed to transition to Federal PKI alternatives by July 2018. After all federal relying parties have confirmed their transition, the ACES PMO will direct the ACES vendor to stop selling/issuing ACES certificates.
    c. The ACES PMO will conduct periodic touchpoints with the federal relying parties to assist with any transition challenges.
C. Phase 3 – Sunset (FY18Q3 – FY20Q3)
    a. Based on the expiration date of the last active ACES certificate, the ACES PMO will monitor sunset status through ACES vendor monthly reporting on remaining active certificates.
    b. Around FY20Q3 when the last ACES certificate is either revoked or expires, the ACES PMO will direct the ACES vendors and the Federal PKI to revoke all ACES CA certificates and decommission the ACES issuing CAs. The ACES PMO will also be decommissioned and program material archived.

Federally Recognized Alternatives

GSA ACES credentials offer two capabilities for authentication and a digital signature for people and device users. In recent years, a number of either federally operated or federally approved options exist. The GSA Identity Management website (https://www.idmanagement.gov/buy/) is a good resource to research current offerings which also include website and vendor contact information. Based on relying party needs, some non-PKI authentication options exist while PKI is the only solution for digital signature. The ACES PMO (ACES-PMO@gsa.gov) is available to answer questions on any alternative options and transition questions.

The Federal Bridge was designed for all partner credentials to be trusted at an equal assurance level and to decrease the need for a business to buy multiple credentials when doing business with multiple agencies.

Figure 1. ACES to Federal PKI Mapping



Federal PKI Alternative Options

The **Federal PKI Non-Federal Issuer (NFI) affiliate program** was designed specifically for businesses to interact with the government in a secure and cost-effective means. A list of Federal PKI Federal Bridge Certification Authority (FBCA) certificate alternatives for each ACES credential is in figure 1. Some advantages of transitioning to NFI affiliates include:

1. Each NFI affiliate is federally recognized through the same compliance process as ACES vendors and also meet NIST assurance level requirements.
2. Increased certificate lifetime of up to three years compared to the ACES two year.
3. Comparable pricing.
4. Higher assurance options for hardware-based credentials (such as PIV-I and medium hardware) not offered by ACES.
5. FBCA Basic and Medium are NIST 800-63-2 level of assurance 3
6. FBCA Medium Hardware and PIV-I are NIST 800-63-2 level of assurance 4

For more information on the NFI program see the Business Identity and Credentials overview on the GSA Identity Management Website (https://www.idmanagement.gov/trust-services/#identity-services). The GSA ACES program was designed specifically for citizens and businesses to purchase individual certificates, and there are NFI affiliates who offer similar services. Table 1 contains a list of NFI affiliates who offer individual certificates.

Table 1. Federal PKI NFI Affiliates Offering Individual Certificates

Affiliate	Contact	Website
IdenTrust	Lorraine Orr (801) 384 3535 (Office) (801) 891 9072 (Mobile) Lorraine.Orr@IdenTrust.com Richard Jensen (801)-384-3514 (Office) (256) 303-9412 (Mobile) Richard.Jensen@IdenTrust.com	https://www.identrust.com/igc/buy.html
ORC	Caroline Godfrey (855) 909-1109	https://www.orc.com/nfi/

While hardware-based credentials (PIV-I or Medium Hardware), managed services, and PKI bridges may be out of reach for an individual, relying parties should recognize all Federal PKI credentials that are comparable to ACES. A federated environment intends to decrease the need for acquiring multiple credentials for connected organizations. Table 2 contains a list of NFI affiliates who offer managed services and PKI bridges for organizations and large communities of interest. Send any questions on credential recognition to GSA-ACES@GSA.gov.

Table 2. NFI Affiliate for Credential Recognition

Affiliate	Contact	Website
Managed Service		
Exostar	Tim Zullo (703) 793 7733	https://www.exostar.com/Identity_Access/Managed_PKI/
Entrust	Dan Miller (703) 346 1164	https://www.entrustdatacard.com/solutions/citizen-id
DigiCert	Kris Singh (801) 701 9642	https://www.digicert.com/fbca-certificates/
PIV-I Provider		
Carillon	Sonny Reid (844) 754 7484	https://pub.carillonfedserv.com/certserv/signup/
SureID	info@sureid.com	https://www.sureid.com/
FTI	Kenneth Boley (210) 704 1650	http://www.foundationfortrustedidentity.org/
PKI Bridge		
CertiPath	Judith Spencer (301) 974 4227	https://www.certipath.com/FederatedTrust_TrustCommunity.html
SAFE-BioPharma	Peter Alterman (301) 943 7452	https://www.safe-biopharma.org/
STRAC	Eric Epley (210) 233 5850	https://pki.strac.org/STRACBridge.html
TSCP	Shauna Russell (202) 769 9114	https://www.tscp.org/

The **Department of Defense (DOD) External Certification Authority (ECA)** program was established to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. Similar to ACES, the ECA program was established prior to many of the commercial PKI partners joining the Federal PKI. ECA certificates are comparable to other FBCA Medium, Medium Hardware, and PIV-I certificates. The exception is DoD ECA relationship is subordinate to the DoD PKI which is subordinate to the Federal Bridge and not directly with the Federal Bridge. More information on the DOD ECA program is available at https://iase.disa.mil/pki/eca/Pages/index.aspx.

ECA Provider	Contact	Website
IdenTrust	Lorraine Orr (801) 384 3535 (Office) (801) 891 9072 (Mobile) Lorraine.Orr@IdenTrust.com Richard Jensen (801)-384-3514 (Office) (256) 303-9412 (Mobile) Richard.Jensen@IdenTrust.com	https://www.identrust.com/certificates/eca/index.html
ORC	Caroline Godfrey (855) 909-1109	https://eca.orc.com/

Non-PKI Alternatives for Authentication

For non-PKI authentication options, two options exist with one operated by GSA.

Organization	Contact	Website	Community of Interest
ID.me	Blake Hall (703) 992-8380	https://www.id.me/	First responders, veterans, teachers, government employees
GSA	hello@login.gov	https://login.gov/	Citizens

Testing Support

Certificate chains for transition testing can be found on either the Federal PKI Crawler website (https://fpki-graph.fpki-lab.gov/crawler/). Sample certificates may be requested directly from NFI affiliates.

NFI Intermediate certificates can be found at http://http.fpki.gov/bridge/caCertsIssuedByfbca2016.p7c.

Additional Resources

GSA and the Federal PKI have a number resources available.

1. Federal Identity Roadmap - https://arch.idmanagement.gov/
2. Federal PKI Guide - https://fpki.idmanagement.gov/
3. PIV / PIV-I Guide - https://piv.idmanagement.gov/
4. Business and Consumer Identity Services - https://www.idmanagement.gov/trust-services/#overview