



DoD PKE Forum eBusiness Track Interoperability Challenges

Rebecca Nielsen
Booz Allen Hamilton



This briefing highlights the requirements, challenges, and processes involved in PKI Interoperability.

- ▶ PKI interoperability refers to the ability of relying parties such as applications and e-mail users to accept digital certificates issued by DoD Approved External PKIs
- ▶ PKI interoperability is distinct from application interoperability which is the ability of applications to properly accept and verify certificates issued by the DoD PKI



Agenda

- ▶ The requirement for interoperability
- ▶ History of interoperability
- ▶ Certificate Policy Mapping
- ▶ Technical Interoperability Challenges
- ▶ Business Model Impact



Although the DoD PKI is issuing Common Access Cards (CACs) to all eligible personnel, many DoD partners require access to DoD Sensitive information.

- ▶ DoD Eligible Users are active duty uniformed services personnel, members of the Selected Reserve, DoD civilian employees, and personnel working on site at DoD facilities using DoD network and e-mail services.
- ▶ DoD Partners are government or non-government entities that process electronic transactions or exchange e-mail containing DoD sensitive information - these entities will require certificates issued by DoD-approved external PKIs.
 - Support contractors who do not work at DoD sites
 - Vendors
 - Members of Allied and coalition forces
 - Employees of other Federal agencies such as the Department of Homeland Security

Implementing interoperability comes with a cost. The DoD manages interoperability decisions so that DoD functional community requirements are met while minimizing the burden on the DoD PKI and PK-Enabled applications.



It's all about trust. Facilitating information exchange between authorized parties while preventing unauthorized disclosure is the goal of interoperability.

- ▶ Who do you trust?
- ▶ How do you know you are dealing with the person you trust?
- ▶ Who do you trust to tell you who you are dealing with?
 - A Public Key Infrastructure is a credential provider
- ▶ Who do you trust to decide who to tell you who you trust
 - The Assistant Secretary of Defense for Network and Information Integration, as the DoD Chief Information Officer, has not delegated the responsibility for approving external PKIs for use within the Department

Authorization

Authentication

Credential Provider

PKI Interoperability



Agenda

- ▶ The requirement for interoperability
- ▶ History of interoperability
- ▶ Certificate Policy Mapping
- ▶ Technical Interoperability Challenges
- ▶ Business Model Impact



The DoD PKI Program Management Office has been evaluating and implementing external PKI interoperability with DoD managed programs and programs external to the DoD.

- ▶ In the beginning...there was the Interim External Certificate Authority (IECA) program
 - Barriers to success included the lack of Public Key (PK) Enabled applications and the difficulty of keeping track of IECA Certification Authority (CA) certificates
- ▶ Then came the Access Certificates for Electronic Services (ACES) program sponsored by the General Services Administration
 - Although significant progress was made in mapping the ACES and DoD Certificate Policy requirements, the DoD determined that technical challenges and the ACES cost model prevented interoperability
- ▶ The DoD PKI was asked to join the Federal Bridge Certification Authority (FBCA)
 - The DoD PKI has achieved one-way interoperability with the FBCA and is still addressing technical and policy issues for two-way interoperability
- ▶ Recently, the DoD PKI sponsored the standup of the External Certification Authority (ECA) with its own Root CA and Certificate Policy (CP)
 - The program architecture builds on lessons learned from other efforts



The determination process for interoperability decisions with these programs centered around policy, technical, and business model questions.

- ▶ Policy questions are identified by mapping the program's Certificate Policy (CP) against the requirements of the DoD X.509 CP
- ▶ Technical questions are identified by assessing
 - Certificate and Certificate Revocation List profiles, especially the use of critical extensions
 - Mechanisms for determining certificate revocation status
 - Application requirements for accepting certificates issued by the external PKI
- ▶ The business model analysis looks at the cost to the DoD PKI and to applications for achieving interoperability versus the requirement for and benefits of interoperating with the external PKI



Agenda

- ▶ The requirement for interoperability
- ▶ History of interoperability
- ▶ Certificate Policy Mapping
- ▶ Technical Interoperability Challenges
- ▶ Business Model Impact



The goal of policy mapping is to determine if the Certificate Policy (CP) that governs the overall operations of the external PKI meets PKI requirements as defined in the DoD X.509 CP.

- ▶ The external PKI CP must meet the assurance level needed for the applications that require interoperability
 - The DoD CP provides requirements for four levels of assurance, Class 2, Class 3, Class 3 Hardware, and Class 4 with associated acceptable use guidelines
 - If the external CP is not fully comparable to the desired level of assurance, the DoD must decide if the risk of accepting certificates from the external PKI is acceptable based on the specific areas of non-compliance
- ▶ The Certificate Policy Management Working Group has primary responsibility for performing compliance analyses against the DoD X.509 CP.

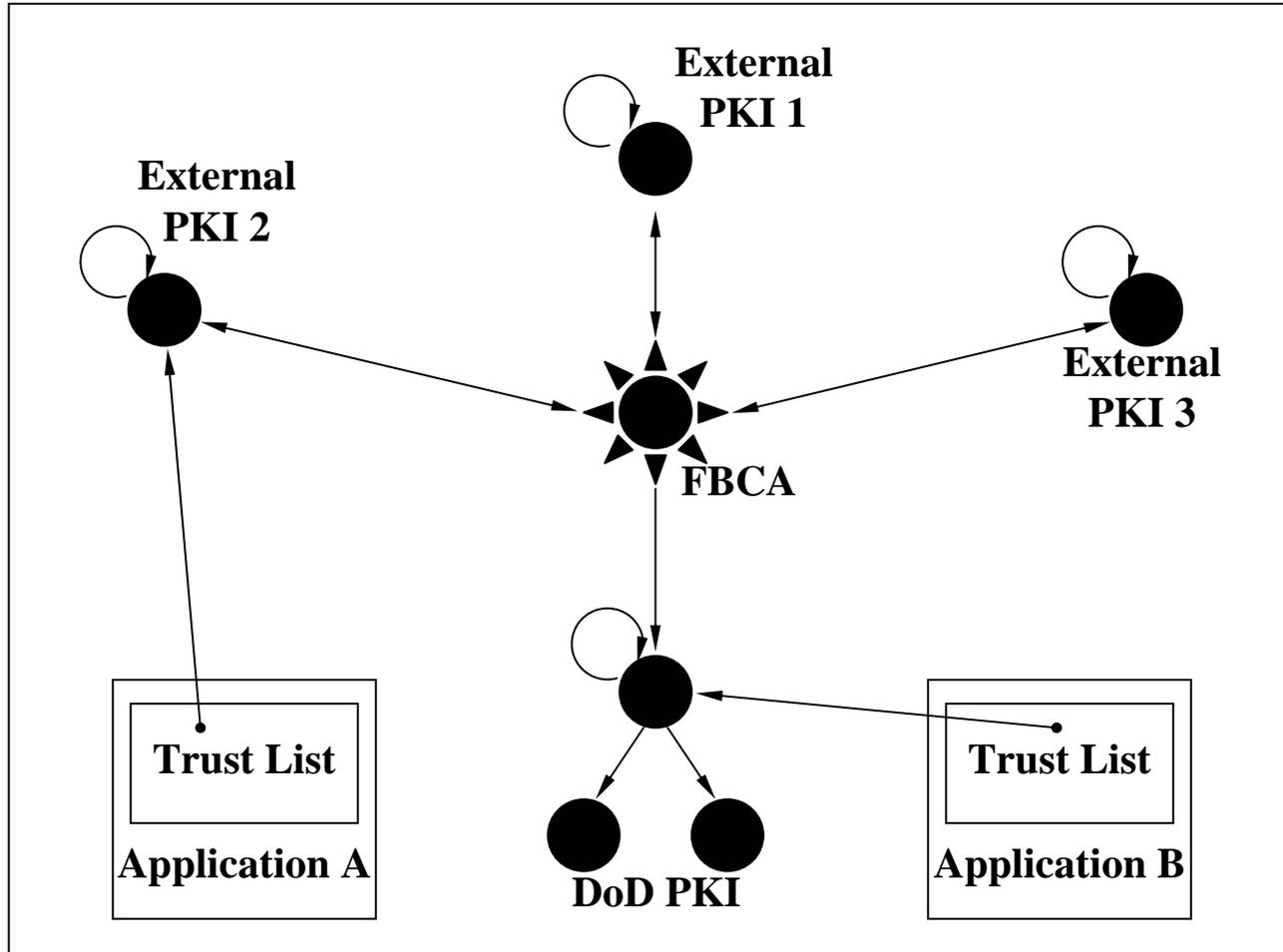


Agenda

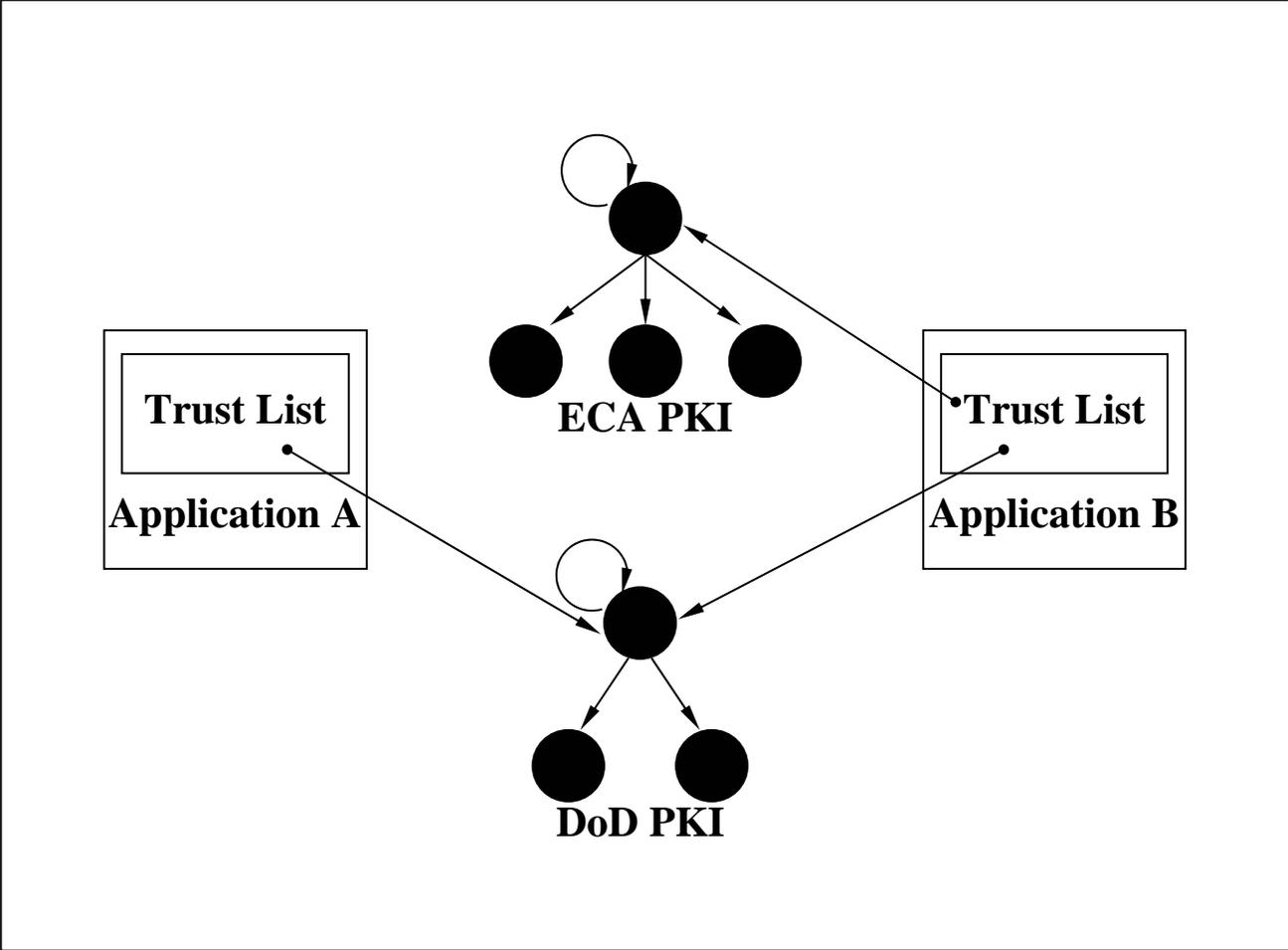
- ▶ The requirement for interoperability
- ▶ History of interoperability
- ▶ Certificate Policy Mapping
- ▶ Technical Interoperability Challenges
- ▶ Business Model Impact



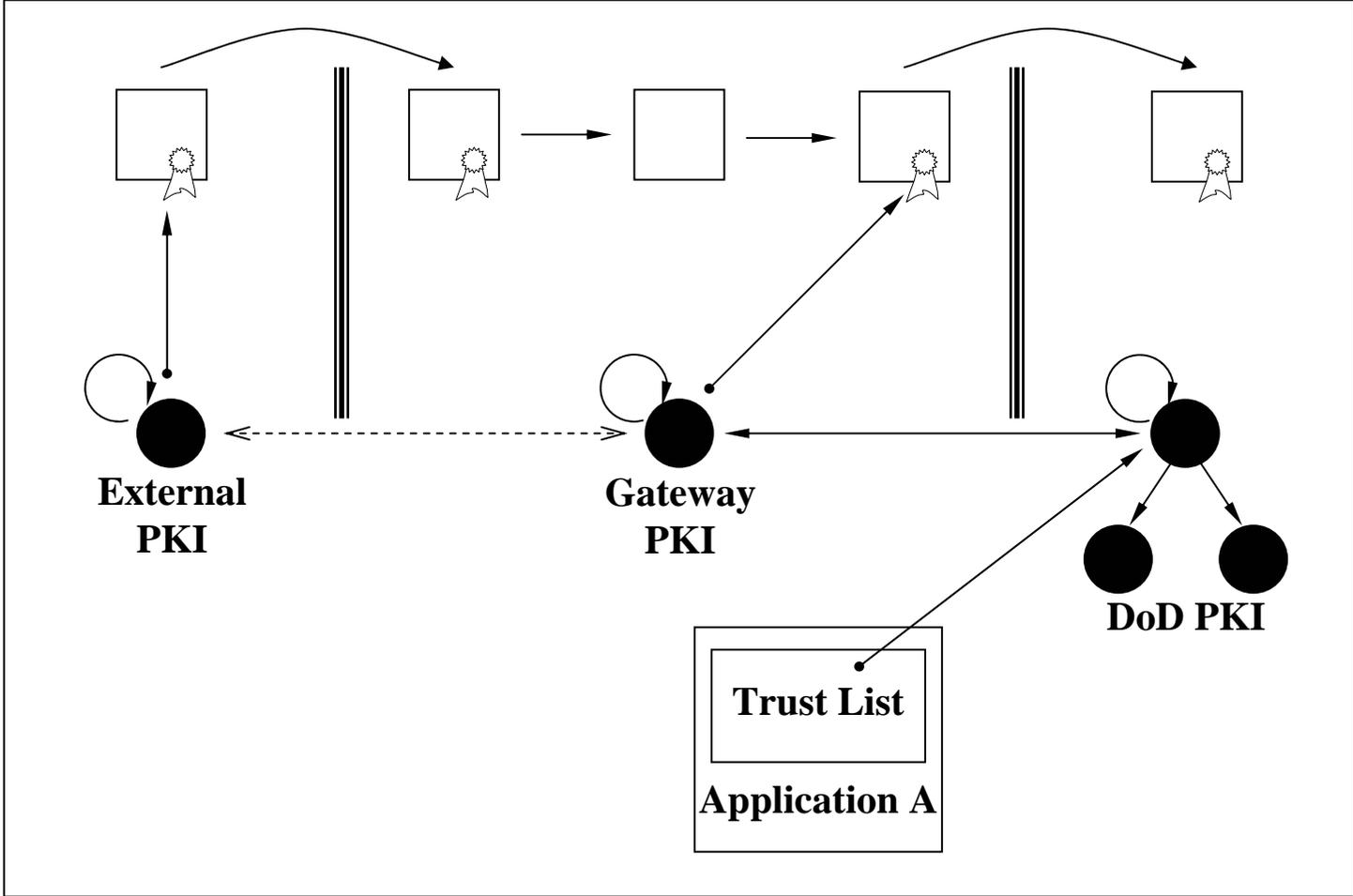
Interoperability can be achieved using different methods. At the CA level, interoperability involves each CA issuing a cross-certificate to the other CA, such as the Federal Bridge.



Applications can implement interoperability directly by adding PKI Certificate Authority certificates into their local trust lists, in accordance with DoD Policy.



When information crosses network boundaries, such as across classifications or countries, a gateway approach can mitigate technical issues or protect the identities of certificate holders.



The decision to extends the boundaries of trust outside of the DoD by interoperating with external PKIs has associated risks.

RISK	METHODS	MITIGATION STRATEGY
Trusting an external entity	<ul style="list-style-type: none"> ▪ CA Level ▪ Application Level ▪ Network Level 	<ul style="list-style-type: none"> ▪ Controls on interoperability process ▪ Monitor audit results
Trusting an external entity to make trust decisions	<ul style="list-style-type: none"> ▪ CA Level ▪ Network Level 	<ul style="list-style-type: none"> ▪ Limit use ▪ Monitor external entity trust rules ▪ Participate on decision board
Improper path processing	<ul style="list-style-type: none"> ▪ CA Level 	<ul style="list-style-type: none"> ▪ Application testing for path processing ▪ Awareness training
Applications managing trust independently of DoD approved external PKIs	<ul style="list-style-type: none"> ▪ Application Level 	<ul style="list-style-type: none"> ▪ Awareness training
Trusting PKI certificates for access control instead of just authentication	<ul style="list-style-type: none"> ▪ CA Level ▪ Application Level ▪ Network Level 	<ul style="list-style-type: none"> ▪ Awareness training ▪ Application reporting requirement for how access control is managed



DoD Public Key (PK) Enabled applications that are accessed by DoD partners must incorporate the capability to accept certificates issued by DoD-approved external PKIs.

- ▶ PK-Enabled application maturity lags significantly behind PKI maturity
 - Web browser clients do not allow users to select certificates issued by CAs not in the application's local trust list
 - Path processing is not uniformly supported
 - Integrating certificates with access control mechanisms is significantly harder than turning on client certificate based authentication
- ▶ Availability of revocation information and ability to manage real time status checking is critical
- ▶ Increasing the number of DoD-approved external PKIs adds to the complexity of an already challenging problem



Agenda

- ▶ The requirement for interoperability
- ▶ History of interoperability
- ▶ Certificate Policy Mapping
- ▶ Technical Interoperability Challenges
- ▶ Business Model Impact



The business model analysis looks at cost issues, including monetary costs, personnel time, and increased risk.

- ▶ Revocation status checking
- ▶ Cost to applications that do not require the external PKI
 - Evaluate the potential impact on applications that will inherit trust in the external PKI but will not rely on certificates from the external PKI
- ▶ Technical operation
 - What will the DoD PKI or relying parties need to implement to accommodate any technical differences
 - The cost associated with initial implementation, deployment, operation, and maintenance
- ▶ Managing trust
 - Issuance of cross certificate pairs and the periodic re-issuance of these certificates
 - Secure delivery and installation of the trust anchor certificate into relying party applications.
- ▶ Maintaining the policy map
 - Changes to the DoD X.509 CP or the external PKI CP must be assessed to ensure that the assurance levels of the two PKIs remain compatible
- ▶ Liability
 - The DoD is not liable for actions of parties external to the DoD
 - The external PKI should be liable for events resulting in the negligence by the external PKI



QUESTIONS?

Rebecca Nielsen
nielsen_rebecca@bah.com
703-902-6985

