

Federated Access Identity & Privacy Protection

Presented at:

**Information Systems Security Association-Northern
Virginia (ISSA-NOVA) Chapter Meeting**

Presented by:

Daniel E. Turissini

**Board Member, Federation for Identity and Cross-
Credentialing Systems (FiXs)**

<http://www.FiXs.org>

January 20, 2011

The Federation for Identity & Cross-Credentialing Systems (FiXS)

- A 501(c)6 not-for-profit trade association formed in 2004 in collaboration with the DoD to provide secure and interoperable use of identity credentials between and among government entities & industry
- A coalition of diverse companies/organizations supporting development & implementation of interoperable identity cross-credentialing standards and systems
- Members include: government contractors, technology companies, major financial firms, not-for-profit organizations, DoD, GSA, state governments, etc.

Federated Identity Solution

- Federated identity provides a strong, biometrically enabled electronic identity credential, that can be readily electronically validated by any Federal logical/physical access point that allows the decision maker or databases to make a local specific privilege and/or authorized ACCESS decision confident in:
 - the identity of the person attempting access;
 - the identity of the device attempting access;
 - the identity of vetted organization that they represent;
 - that the organization and the individual have a legal relationship to do business with the federal government; and,
 - that the individual has been vetted in person and has undergone a background investigation consistent with defined levels.

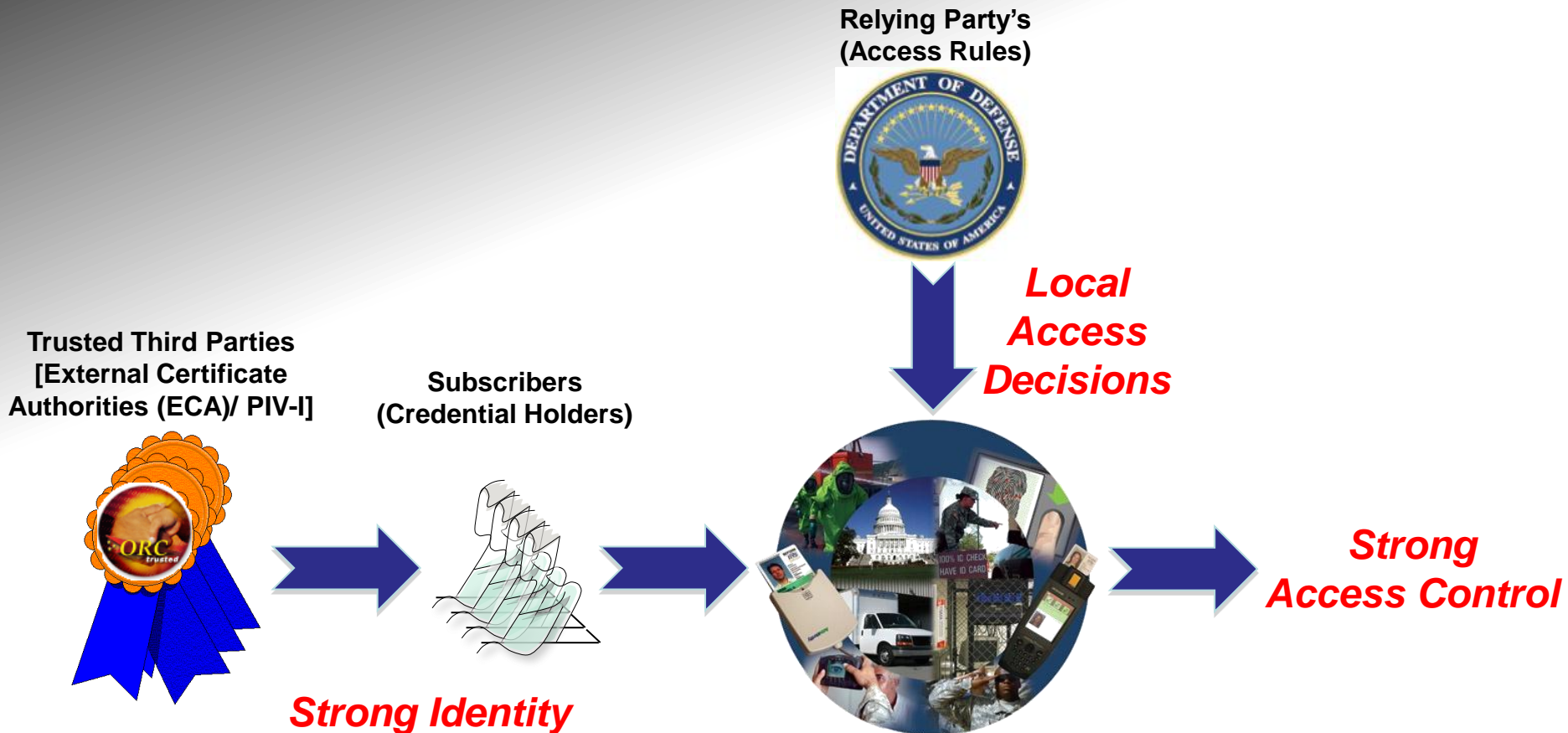
***Credential assures you are who you say you are,
Commander's confirm what holder is permitted to access!***

The Foundation

- FiXs entered into formal Memorandum of Understanding (MOU) with the DoD that established terms & conditions under which FiXs & DoD will use their respective systems as part of an identity suite of systems in January 2006, updated February 2009:
 - <https://www.dmdc.osd.mil/dmdcomn/owa/DMDC.FEDPIIPS>
- The terms and conditions include:
 - Operational framework for inter-operability between DoD & FiXs
 - Specific operational responsibilities
 - Governance structure
- Authority To Operate Granted by DMDC
- Strong Certification & Accreditation Processes

Documentation available online at: <http://www.fixs.org/library>

Federated Access DoD Application



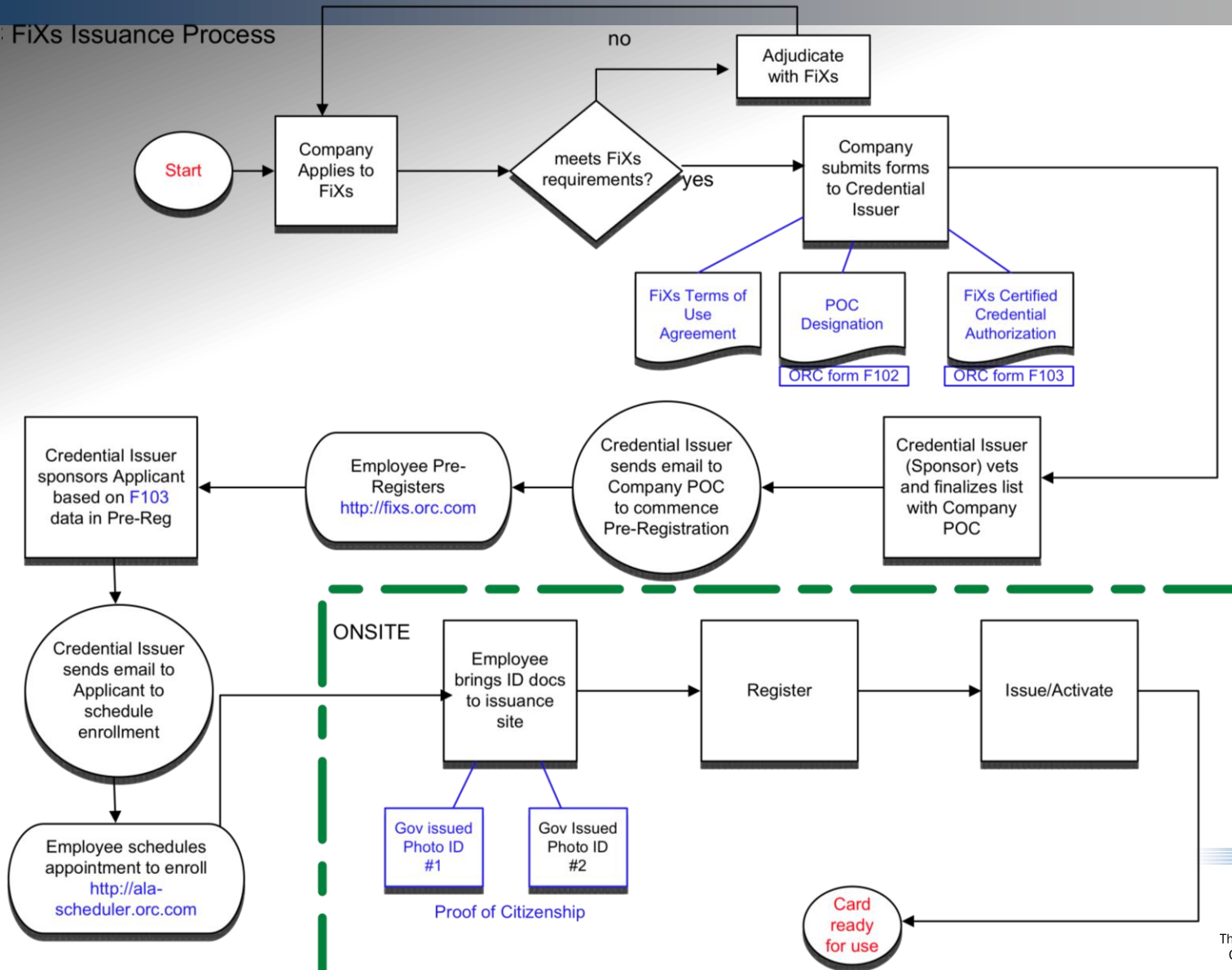
Strong credentials with biometrics consistent with federal standards are essential to successful Access control

TESTED, SPOT – FiXs Inter-operability Pilot

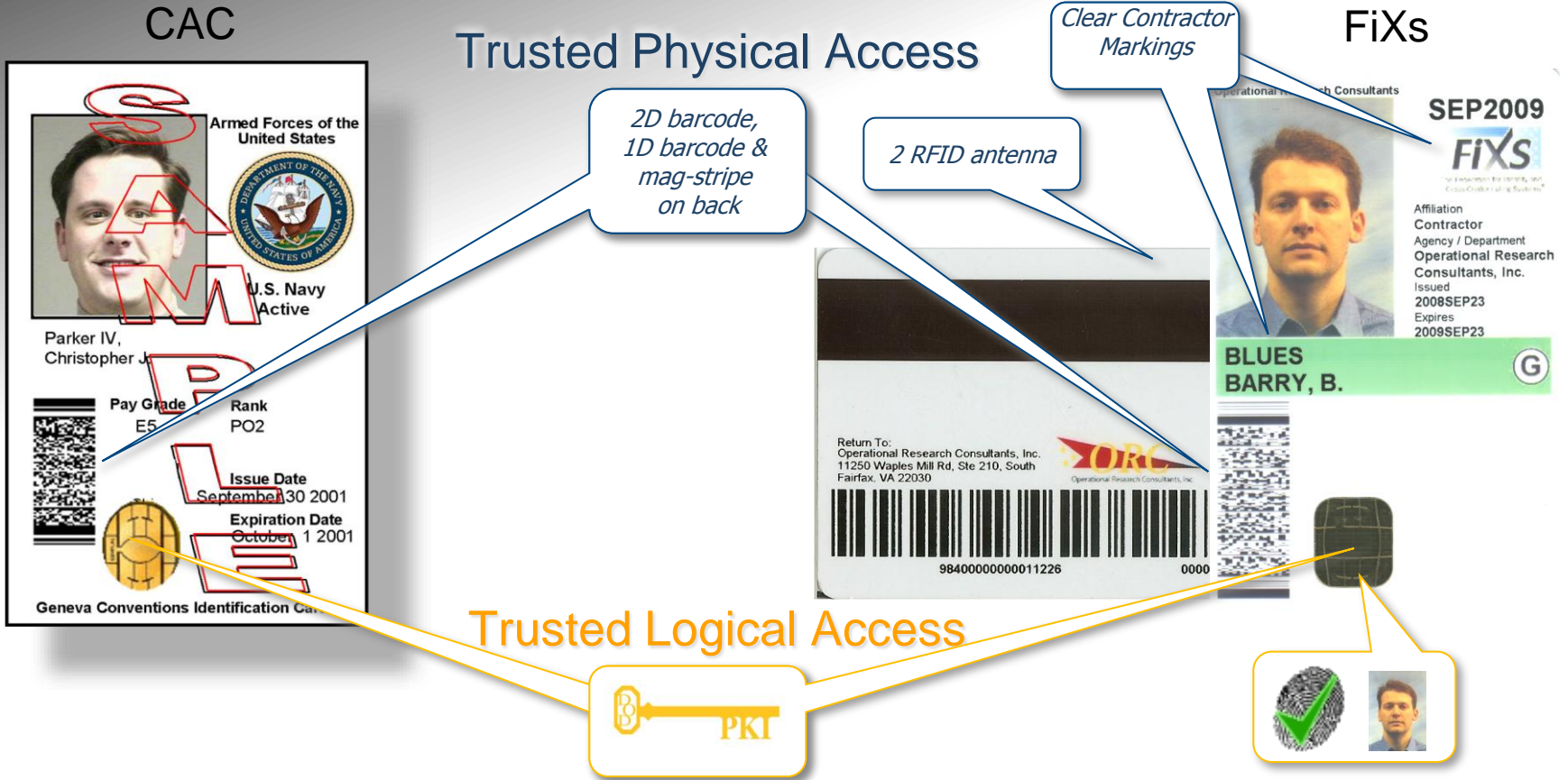
- Successful assessment of the feasibility to utilize commercially - issued credentials in “feeding” the SPOT database – that adhere to FiXs-certified standards
- Issue FiXs-certified credentials - 3,000 contractor personnel
- Credentials authenticated across secure network against federated data stores
- Included “cleared” personnel, non-cleared personnel, first responders, other entities that interact with Army Material Command
- Monitor utilization, increases in productivity, & security profile
- Provided strategic assessment for future activities

FiXs – Chain of Trust

FiXs Issuance Process

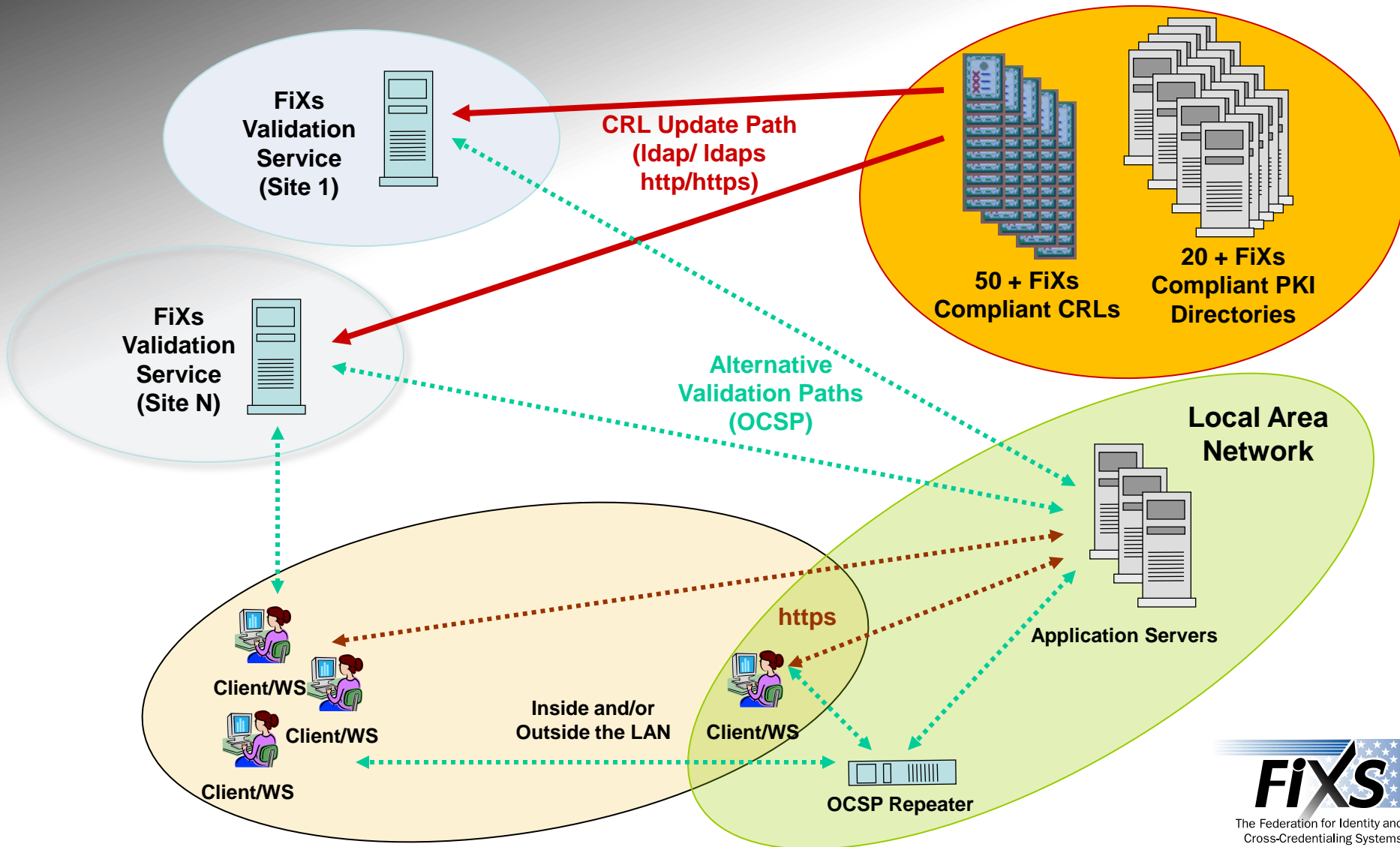


FiXs - Certified Credentials



RFID, Barcodes, PIV Applet and Certificate Provide Issuer ID, Sponsor ID, Employee ID, & other Data Processed via Network

Robust Validation Infrastructure



Device Credential Issuance Process

STEP 1: Apply
Device Administrator goes to any-CA.ORG.com & completes online certificate registration application.



STEP 2: Submit
The device's key pair is generated in a cryptographic module, associated to device & the device's public key is submitted to the CA along with the application.

STEP 3: Print
Administrator prints or PDFs the application form.



STEP 4: ID Proofing
Administrator digitally signs the form & sends or takes the form with two valid forms of ID either to LRA or other Trusted Agent.



STEP 6: Issuance
An CA issues the certificate & provides out-of-band download instructions to the applicant.

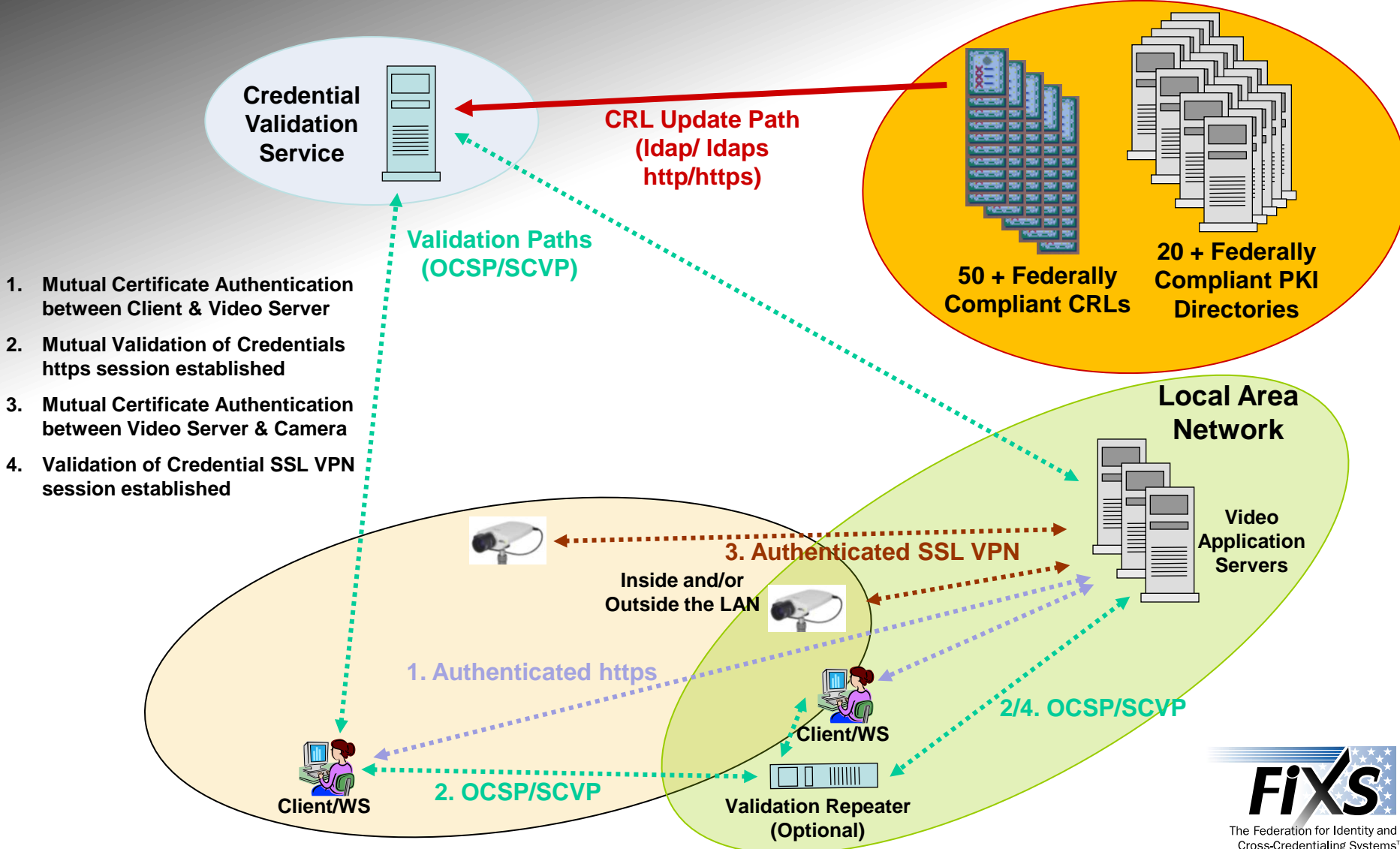
STEP 5: Confirmation
RA confirms that ID proofing is complete & correct.

STEP 7: Download
Administrator returns to any-CA.ORG.com, performs a proof of possession, & downloads their certificate.

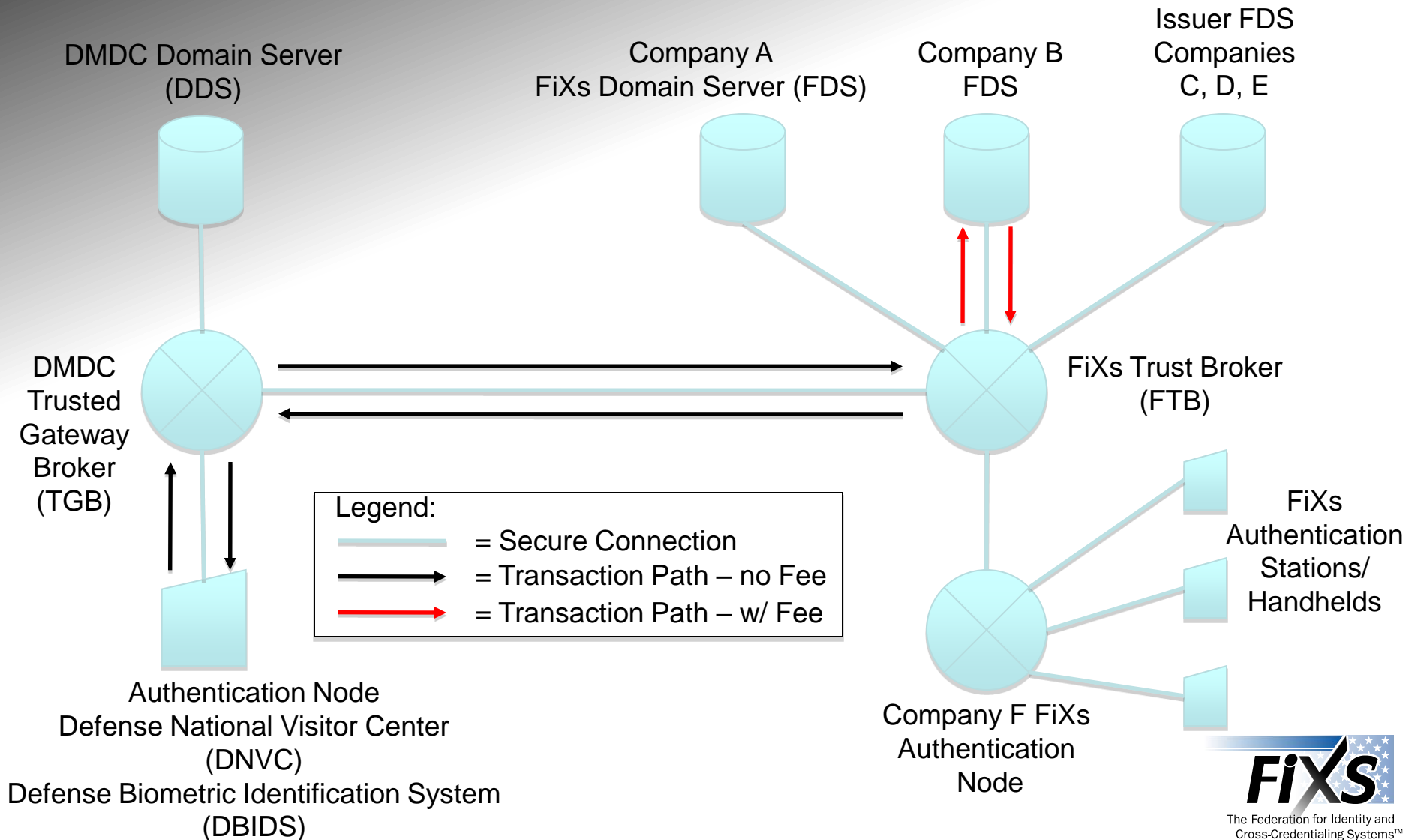
STEP 8: Install
Administrator installs SD into device & applies tamper evident tape.



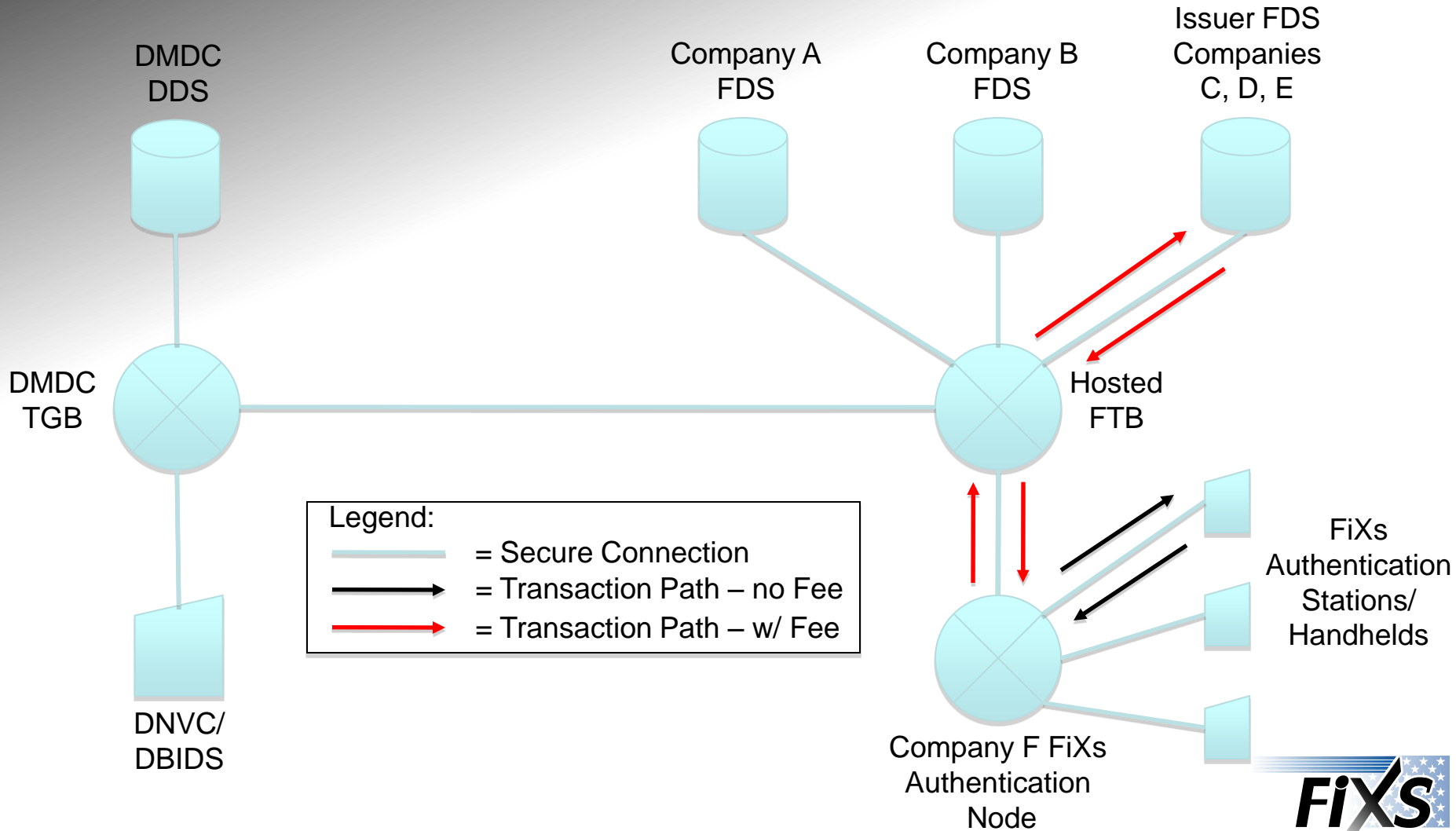
Device Secure Access



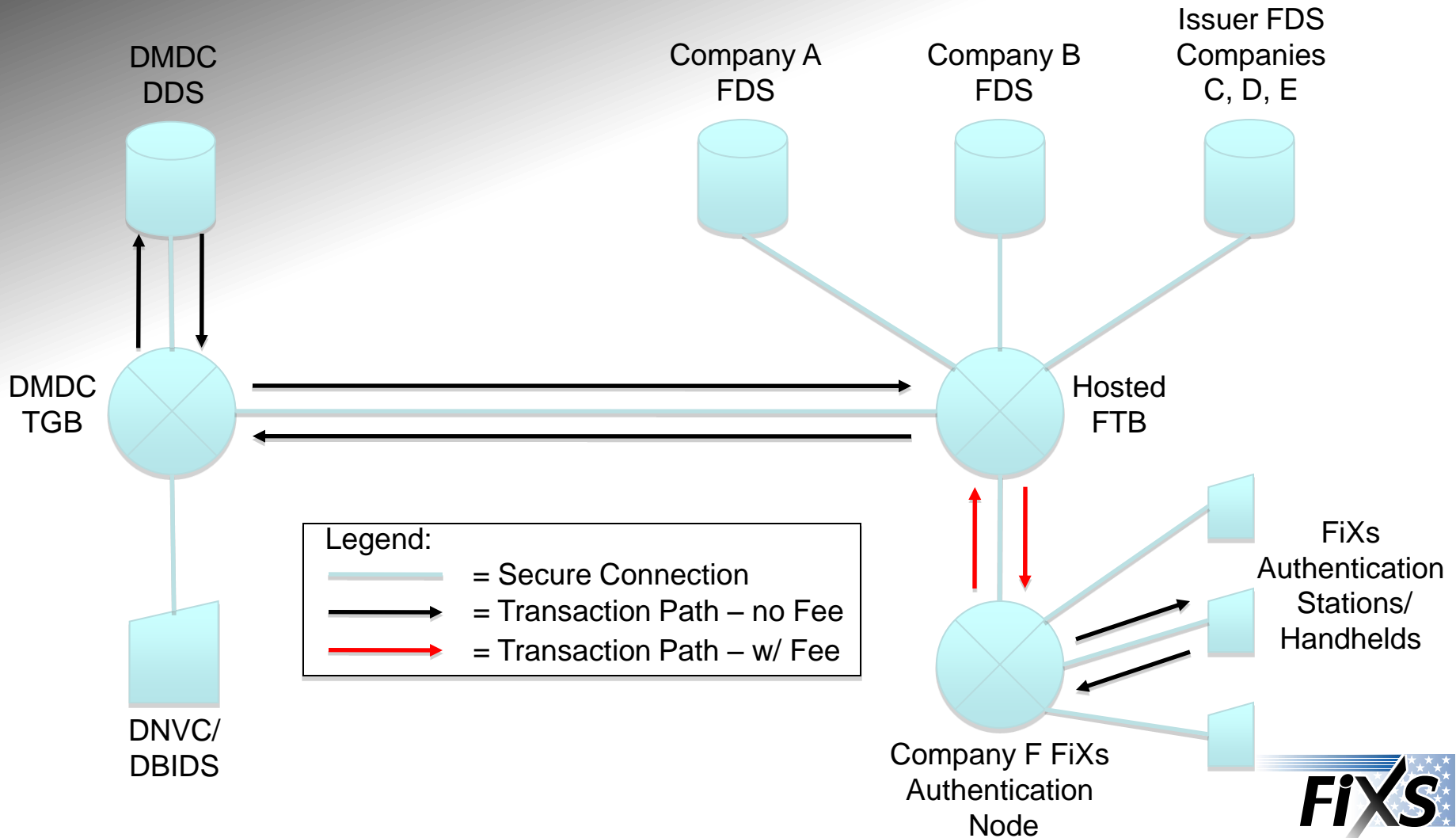
FiXs Certified Credential Authenticated at DoD Location



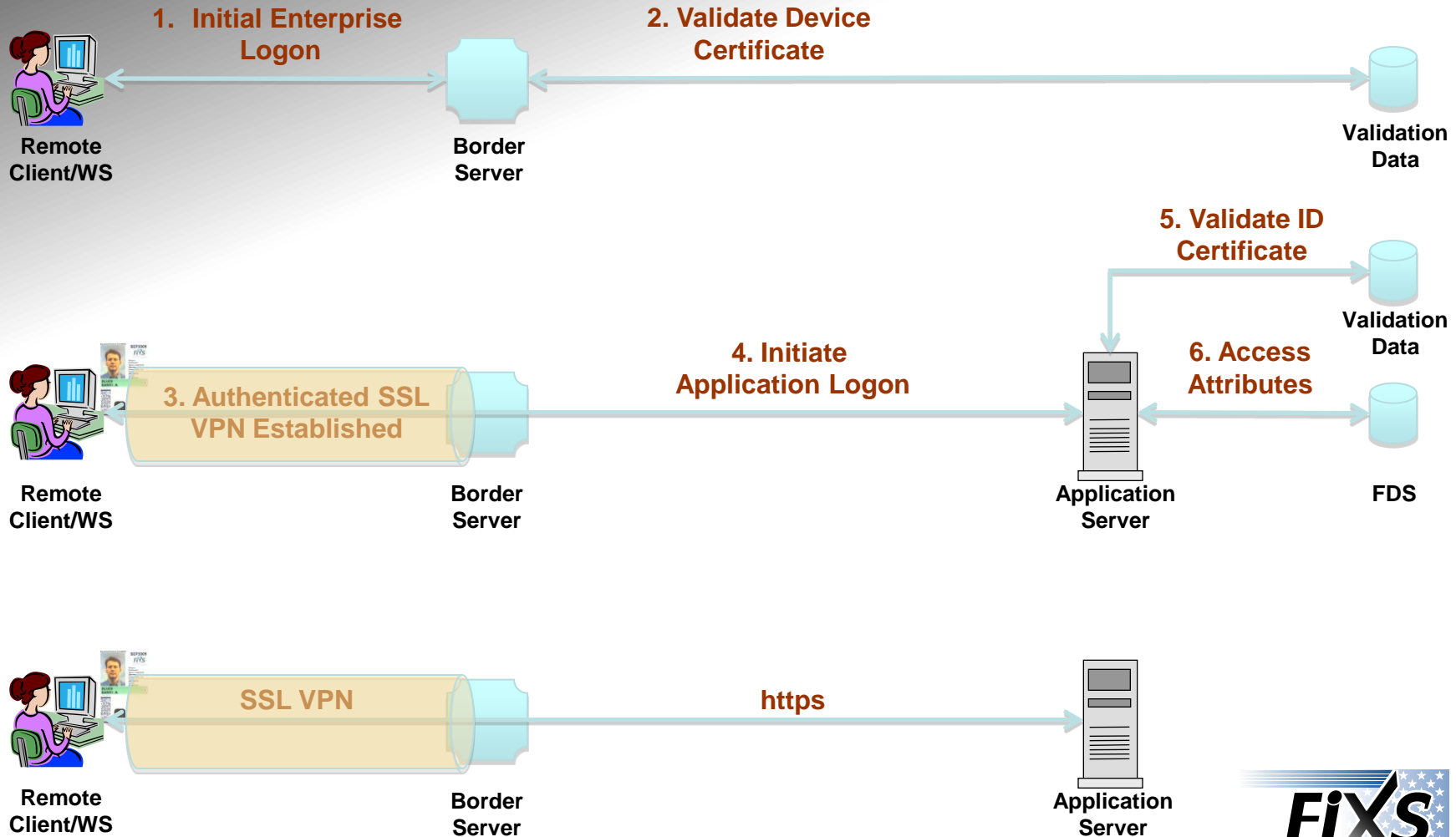
FiXs Certified Credential Authenticated at FiXs Location



CAC Authentication at FiXs Location



FiXS Certified Credential Enhanced Logical Access Control



Contact Information

Dan Turissini - CTO, WidePoint Corporation, FiXs Board

turissd@orc.com

703 246 8550

Dr. Michael Mestrovich, FiXs President

Michael.Mestrovich@fixs.org

703 928 3157