authenticate 2022
THE FIDO CONFERENCE

Case Study: Enterprise PIV-authentication sans Active Directory!

Dr. Sarbari Gupta, CISSP, CISA
Founder & CEO, Electrosoft (www.electrosoft-inc.com)
https://www.linkedin.com/in/sarbari-gupta/

Sponsored by:
Google | Microsoft | yubico | VISA

authenticatecon.com

Agenda

- Background and Problem Statement
- Solution Options
- Solution Implementation Details
- Support for Agency Use Cases
- Solution Summary

Electrosoft

Background and Problem Statement

Executive Order 14028

- **Modernizing Federal Government Cybersecurity**
  - Prioritize adoption and use of cloud technology
  - Develop a plan to implement ZTA
  - **Adopt MFA** and Encryption for data at rest
  - Identify sensitive unclassified data
- **Challenges for Small/Micro Agencies**
  - Lack Budget
  - Lack Skilled IT Staff
  - Lack IT Security Staff

THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But

Electrosoft

Agency Goals for Alignment with EO 14028

- **Mandatory PIV*-based authentication to Agency-owned workstations**
- **Alternate MFA solution when PIV is unavailable**
- **Low cost to administer and operate**
- **Secure, cloud-based solution**

Personal Identity Verification – Smart Card identity credential issued to all Federal staff based on FIPS 201 standard

Electrosoft

Personal Verification Card (PIV) Card Basics

- US Federal Government Smart Card Identity
- Based on FIPS 201 Standard
- Strong Identity Proofing and Issuance
- Includes 4 PKI credentials
  - Authentication
  - Digital Signature
  - Encryption
  - Card Authentication
- Includes biometrics (fingerprints,facial image)
- Activation with PIN or biometric (optional)

Source: fedidcard.gov

Electrosoft

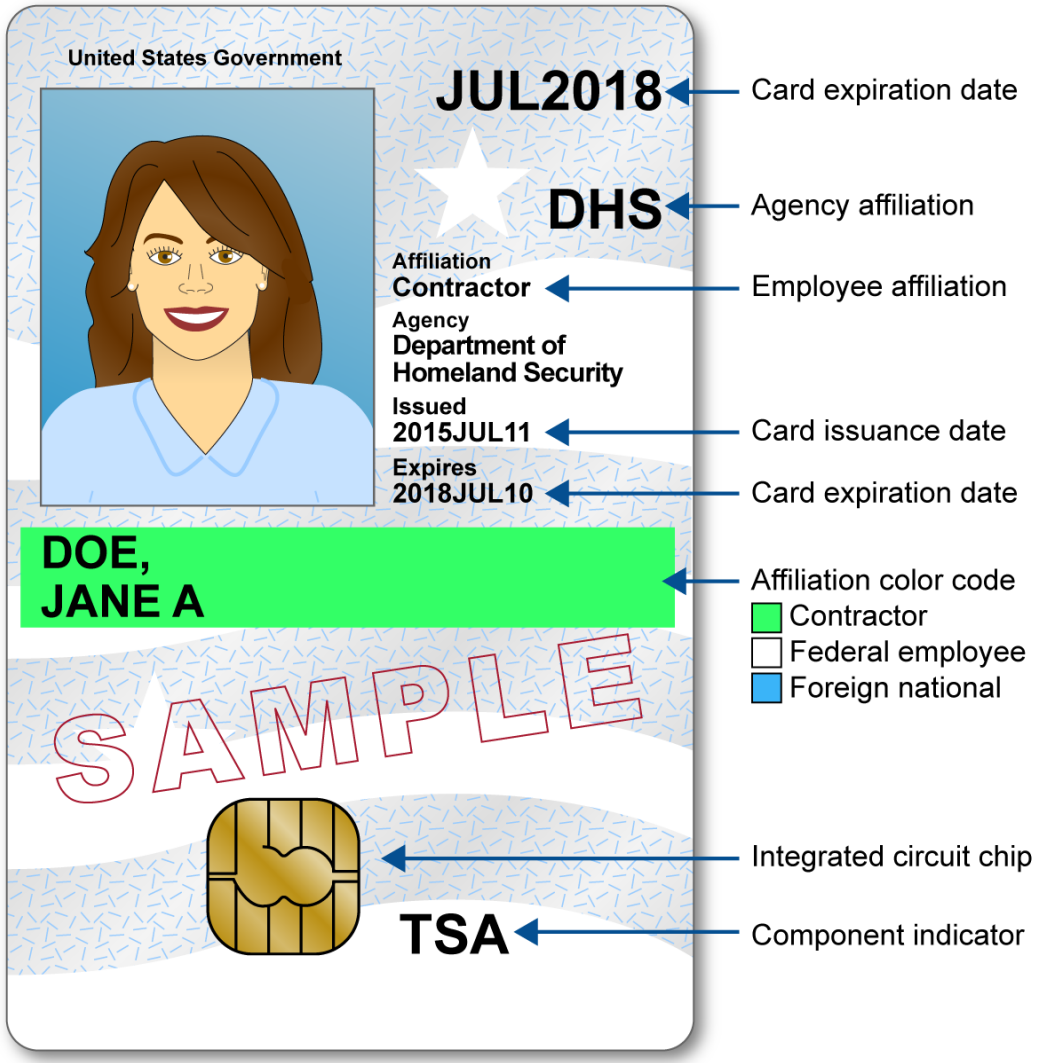
Agency IT Environment

- **Micro-Agency**
  - Less than 100 staff spread throughout the USA
- **Each Staff has Agency-Issued Win 10 Laptop**
  - Not connected to AD or Azure AD (i.e., standalone)
  - User logs on using local user account
  - Administered through remote admin tools and local admin accounts
  - Laptops shipped back to HQ for some admin tasks
- **Agency currently 100% in the Cloud**
  - Cloud-based Workspace for Email, Storage & Collaboration
  - Multiple SaaS applications
  - Limited IT and IT Security Staff

Electrosoft

Agency PIV Card Status

- **PIV Cards issued through GSA USAccess (www.fedidcard.gov)**
- **Most staff members have been issued a PIV Card, however:**
  - Some staff do not have PIV Cards
  - Some staff have expired PIV Cards
  - Many PIV Card holders have forgotten their PINs
- **Agency has not integrated PIV Cards for physical or logical access**



Source: GAO. | GAO-19-138

Electrosoft

Solution Options

Option One - On-Prem Active Directory (AD)

- **Pros:**
  - Leverages Microsoft Smart Card Logon functionality
  - Enables Mandatory PIV-authentication to end points
  - Supports Group policy management
- **Cons:**
  - Moves Agency back into on-premise IT implementation
  - Expensive to operate (continuing administrative support costs)
  - Significant security authorization costs (security control implementation, assessment and continuous monitoring)

Electrosoft

Option Two - Azure Active Directory (AAD)

- **Pros:**
  - Aligns with Agency Cloud Strategy
  - Enables Mandatory PIV-authentication to end points
  - Supports Group policy management
- **Cons:**
  - Disruption (due to change from current environment)
  - Complex to implement for this micro-agency (transition costs)
  - Expensive to operate (license and administrative support costs)
  - Significant security authorization costs (security control implementation, assessment and continuous monitoring)

Electrosoft

Option Three – Cloud-based (SaaS) IAM Solution

- **Pros:**
  - Aligns with Agency Cloud Strategy
  - Single Enterprise Cloud Directory for all Identities (internal and external)
  - Enables desktop SSO to other Agency Applications / SaaS services
- **Cons:**
  - Requires additional products (such as TechMFA) for MFA login to standalone laptops
  - Often very expensive

Electrosoft

Option Four - Desktop Smart Card Authentication Agent + Backup MFA via SaaS

- **Pros:**
  - Aligns with Agency Cloud Strategy
  - Maintains current non-AD environment at Agency
  - Enables Mandatory PIV-authentication to Agency End Points
  - Provides backup MFA solution when PIV is unavailable
  - Very Economical (compared to other solutions)
  - Requires minimal effort to obtain security authorization
- **Cons:**
  - Integrated solution based on two separate products/services
  - Implementation is manual and a bit tricky

Solution Implementation Details

Selected Solution – Option 4

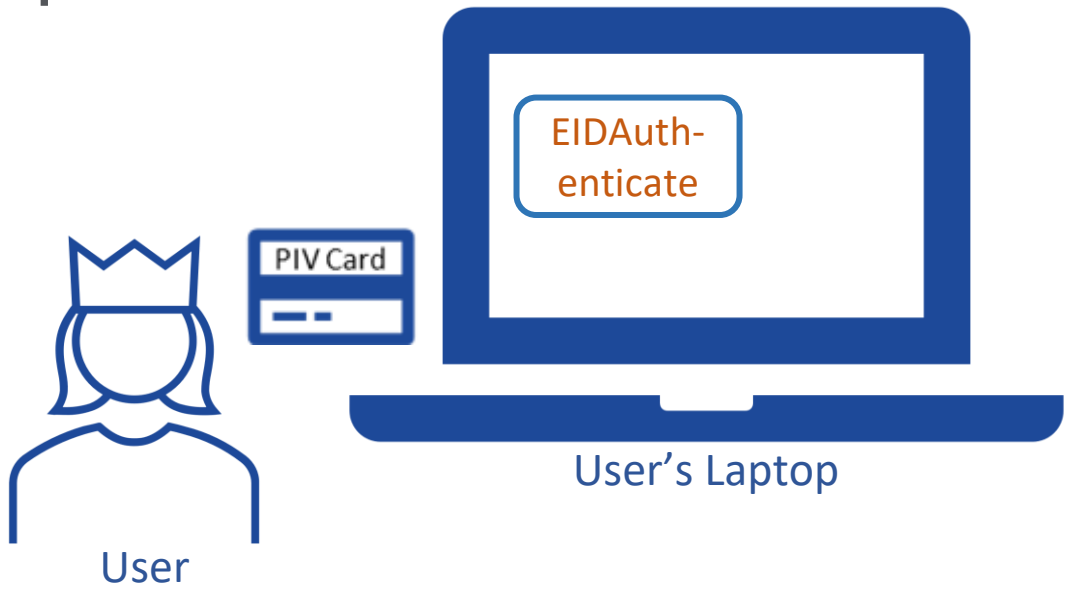
- **Technical Components**
  - MySmartLogon EIDAuthenticate Credential Provider
  - Duo Federal MFA Solution (SaaS) and Duo Win Logon Client

- **Procedural Components**
  - Processes for Setup and Management of Technical Components to support Agency Use Cases

Electrosoft

MySmartLogon EIDAuthenticate Configuration

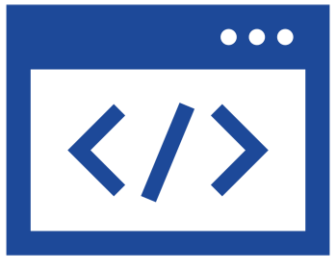
- **Install EIDAuthenticate credential provider on each User Laptop**
- **Configure to require PIV authentication for User**
  - Associate with User's PIV-AUTH certificate
  - Associate with User's local account on laptop
- **Configure PIV Card Validation details**
  - Test authentication success using User's PIV-AUTH certificate
  - Configure to check PIV Card revocation status **only** when connected to Internet



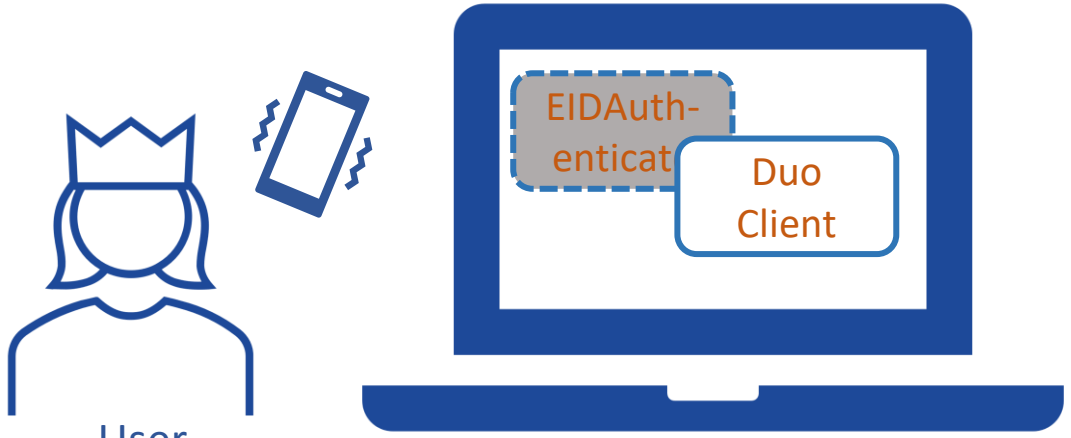
Electrosoft

Duo Federal SaaS and Duo Win Logon Client Configuration

- **Require each User to enroll in Duo Federal SaaS with MFA**
  - Password and Second factor (SMS, Authenticator App, phone, etc.)
- **Install Duo Win Logon Client on each User Laptop**
  - Connect with Agency's Duo Federal SaaS Portal
  - Configure to require MFA for both regular and administrative user accounts
  - Configure to work alongside EIDAuthenticate
- **Set User Account Status on Duo SaaS Portal to drive behavior of Duo Client:**
  - "Disabled" Status
    - Duo Client senses "Disabled" status and is dormant
    - EIDAuthenticate takes control of user login via PIV Card
  - "Active" Status
    - Duo client senses "Active" status and takes control of user login via Duo MFA
    - EIDAuthenticate is dormant
- **All Duo user accounts are set to "Disabled" by default!**
  - All Duo Administrator accounts are set to "Active"



Duo Portal



Electrosoft

Support for Agency Use Cases

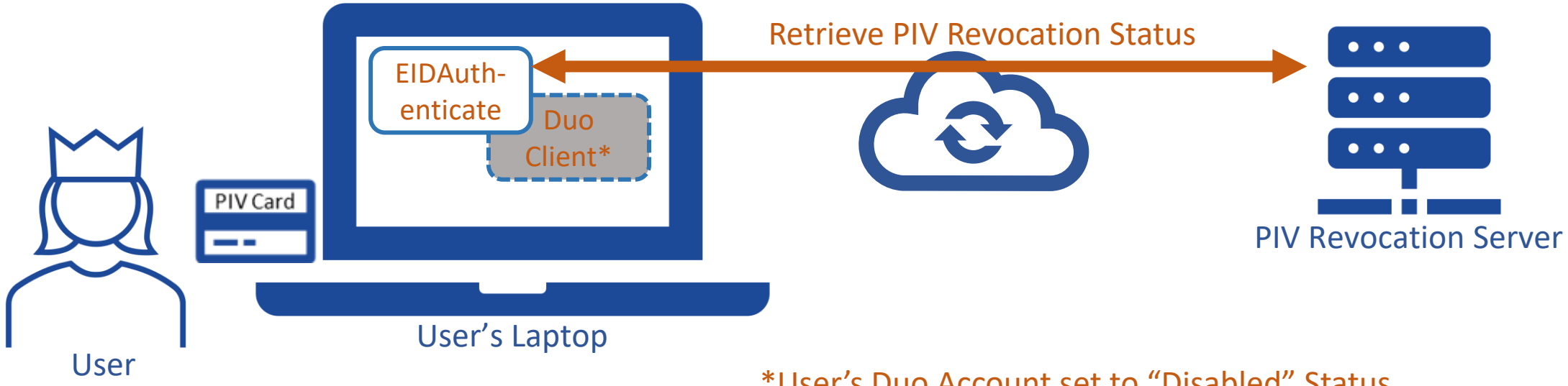
Agency Use Cases

- **User Login to Agency Laptop**
  - #1 – User has PIV Card, Internet Available
  - #2 – User has PIV Card, Internet Unavailable
  - #3 – User's PIV Card Unavailable (lost/broken/forgotten PIN)
  - #4 – User's PIV Card Unavailable and User forgot local account password
- **User Login to Shared Workstation**
  - #5 – User has PIV Card, Internet Available

Electrosoft

Use Case #1: User has PIV Card, Internet Available

- **Normal daily use case for Agency Users that possess working PIV Card**
  - User's account status is set to "Disabled" on Duo SaaS Portal (*default*)
- **User inserts PIV Card into reader**
  - EIDAuthenticate prompts User to provide PIN
  - User authenticates using PIV Card (PIV-AUTH certificate)
  - EIDAuthenticate performs certificate validation checks
  - EIDAuthenticate checks revocation status of PIV Card via Internet

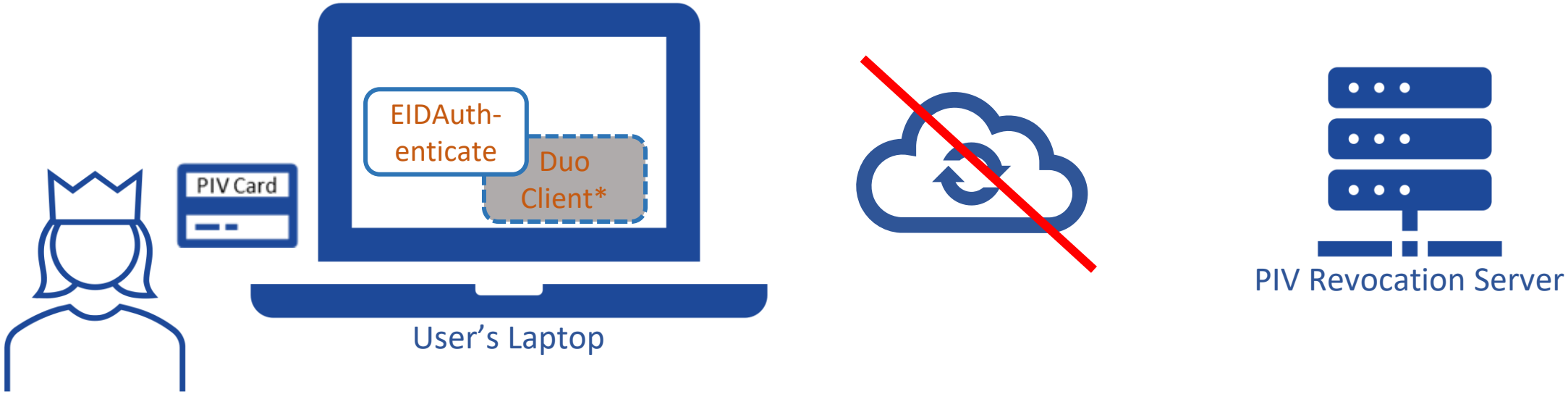


*User's Duo Account set to "Disabled" Status

Electrosoft

Use Case #2: User has PIV Card, Internet Unavailable

- **User and Laptop are in environment with no Internet access**
  - User's account status is set to "Disabled" on Duo SaaS Portal
- **User inserts PIV Card into reader**
  - EIDAuthenticate prompts User to provide PIN
  - User authenticates using PIV Card (PIV-AUTH certificate)
  - EIDAuthenticate performs local validation of PIV Card
  - EIDAuthenticate bypasses PIV revocation check if Internet is unavailable

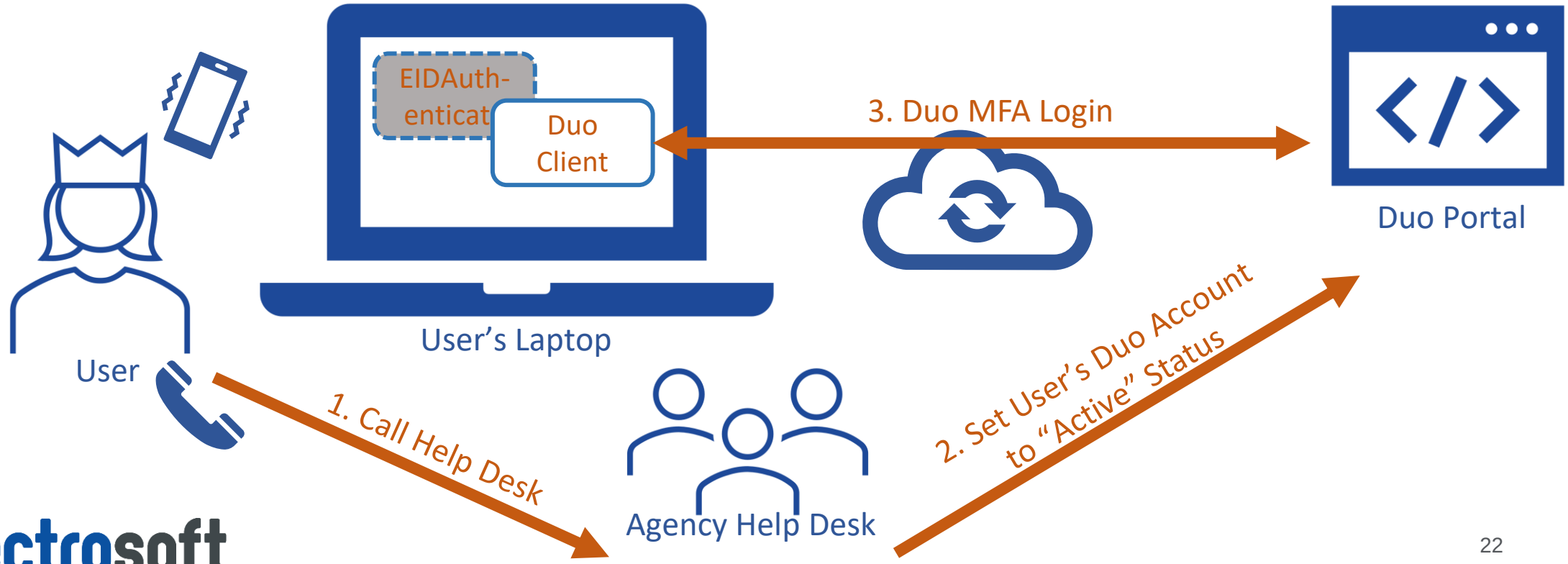


*User's Duo Account set to "Disabled" Status

Electrosoft

Use Case #3: User's PIV Card Unavailable, Internet Available

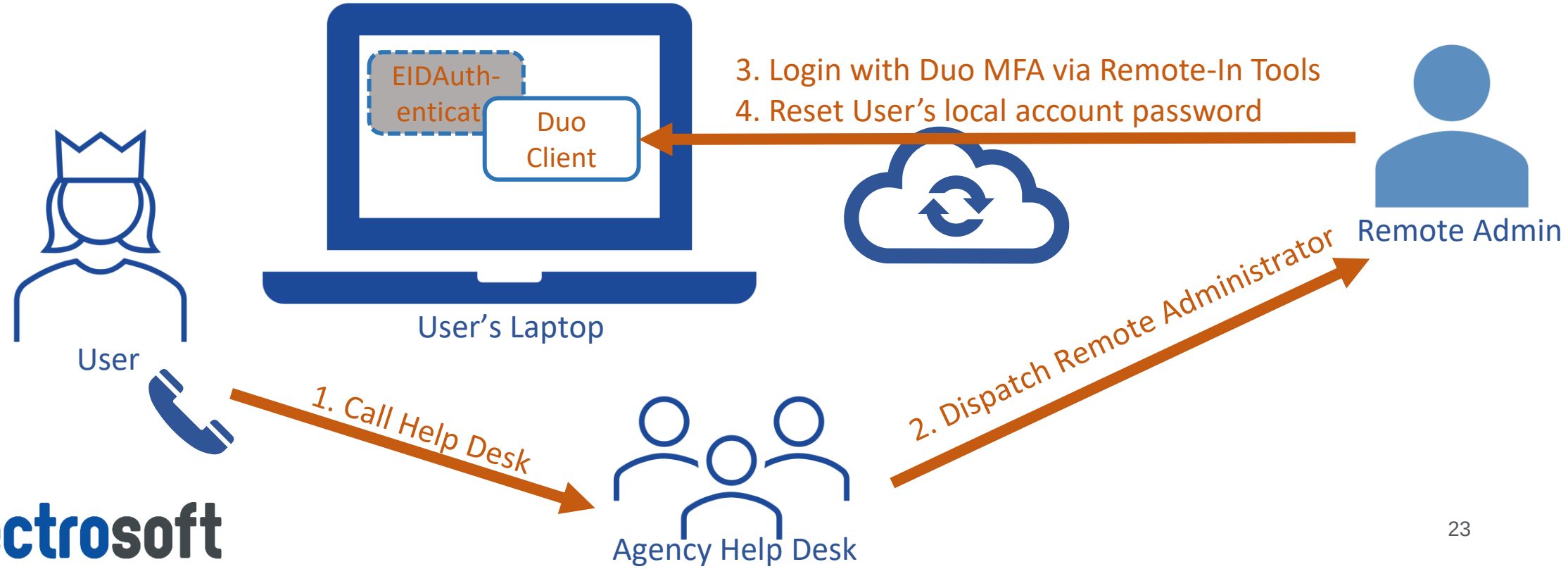
- **User cannot use PIV Card (left at home, lost, broken, forgot PIN)**
  - User calls Agency Help Desk requesting their Duo account be set to "Active"
- **Duo Client senses "Active" status and prompts user for Duo MFA login**
- **User's Duo account set back to "Disabled" based on Agency policy**



Electrosoft

Use Case #4: User's PIV Card Unavailable, User forgot local account password

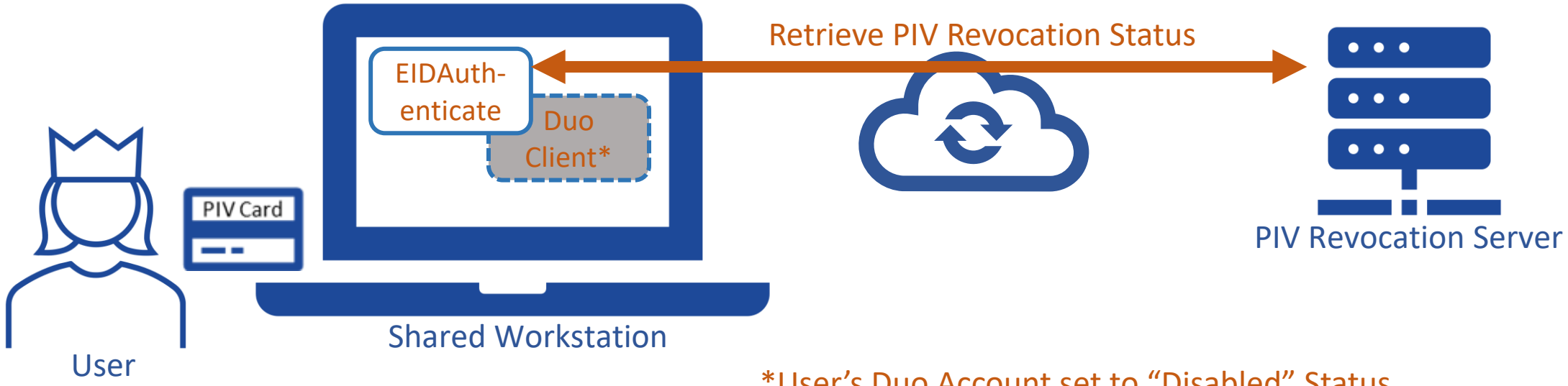
- User calls and requests Agency Admin support to help with login
- Remote Admin connects to User Laptop using remote admin tools
  - Logs in to local admin account using Duo MFA
  - Resets User's local account password
- User proceeds to login using MFA as in Use Case #3



Electrosoft

Use Case #5: User Login to Shared Workstation

- **Each Shared Workstation configured to support local user accounts for all users that may use the workstation**
  - **EDIAuthenticate and Duo Client configurations**
- **User proceeds as in Use Case #1 to login to workstation**



*User's Duo Account set to "Disabled" Status

Electrosoft

Solution Summary

- **Major Strengths**
  - All Agency Workstations configured for mandatory PIV-authentication
  - Backup MFA solution for PIV-unavailable situations
    - No need to issue temporary access cards to such users
  - Improved Remote Administration
    - Remote Admins require MFA
    - Remote reset of local user passwords instead of shipping back to HQ
  - Improved security with low additional workload
    - FedRAMP Authorized Cloud SaaS solution
  - Little disruption to existing work/collaboration environment
  - Scalable, cost-effective – fits smaller budgets
- **Weaknesses**
  - Workstations have to be managed and updated individually with remote administration tools (cannot push out group policies across the enterprise)

authenticate 2022

THE FIDO CONFERENCE

Thank you.

Sponsored by:

Google | Microsoft | yubico | VISA

authenticatecon.com