

**IDENTITY DEVICES FOR****REMOTE AUTHENTICATION**

**Identiv helps organizations validate users via multi-factor authentication before accessing networks, systems, and applications.**

Organizations are realizing the benefits of a remote workforce, including increased savings, easier access to top talent, increased productivity, and reduced turnover.

However, a remote workforce creates other challenges for IT teams. How do you ensure that only your employees have access to your network, systems, and applications?

Identiv's product suite of identity devices and smart card readers for logical access control offers a wide range of options to assist businesses and agencies with secure network log-in for their remote users.

### **Identity Devices Suite**

- RFID, NFC, proximity, and contactless smart card readers
- uTrust FIDO2 Security Keys
- uTrust Token Family
- Contact smart card readers
- Mobile smart card readers
- uTrust TS Cards
- uTrust MD Smart Cards
- uTrust Proximity Credentials

### **Use Case: Department of Defense and HSPD-12**

Identiv has been the leading smart card reader supplier to the Department of Defense (DoD) and federal government since the inception of HSPD-12, enabling CAC and PIV card holders both local and remote authentication.





## Stop cybercriminals in their tracks, resist phishing attacks, and protect user credentials from being compromised.

Passwords are vulnerable no matter how you look at it. But most people increase the chances of having their credentials compromised by reusing the same password or by choosing passwords that are easily remembered. Reports show that employees reuse a password on an average of 13 times, making phishing attacks more effective. Identiv's uTrust FIDO2 Security Keys are small devices that provide the user with phishing-resistant security.

uTrust FIDO2 Security Keys are engineered using FIDO standards that utilize public cryptography to provide strong authentication. Register their uTrust FIDO2 Security Key with hundreds of services that have already adopted FIDO standards (i.e., Gmail, Salesforce, Facebook, and Instagram), remove the need to type in passwords, and provide strong authentication to ensure their credentials are not compromised.

### uTrust FIDO2 NFC Security Keys



### uTrust FIDO2 GOV Security Keys



### Use Case: Secure Remote Access for Employees

Identiv's uTrust FIDO2 Security Keys allow organizations to deploy a scalable, cost-effective, strong authentication solution that ensures that only their employees have access to the corporate applications.





## Identiv technology works with Apple and Android to provide strong security for enterprise and personal mobility.

Technology is constantly evolving, as is the threat to organizations. The effects of each commercial data breach are being felt around the world and costing companies billions of dollars in funds applied to ransomware, post-breach recovery efforts, and lawsuits.

Global attacks highlight the need to increase network security through initiatives such as replacing passwords, which are relatively easy to hack, with two-factor authentication, which is nearly impossible.

Identiv offers government-certified secure applications that are accessed using smart cards, including CAC and PIV. Our most popular application is Thursby Software Systems' Sub Rosa, a secure mobile web browser application available for Apple and Android mobile devices, which uses multi-factor authentication paired with our smart card readers. Sub Rosa allows end-users to securely browse sites, including those that require security certificates, access Outlook Web App (OWA), sign, encrypt, and decrypt email, and sign PDFs on-the-go or while working from home.



Identiv's mission is to secure access to the connected physical world: from perimeter to desktop access, and from the world of physical things to the Internet of Everything.

[identiv.com](http://identiv.com) // +1 888-809-8880 // [sales@identiv.com](mailto:sales@identiv.com)