yubico

# Achieving Level of Assurance 3 and 4 with YubiKeys

## White Paper

**June 16, 2016**

## Copyright



## Trademarks

Yubico and YubiKey are trademarks of Yubico Inc. All other trademarks are the property of their respective owners.

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

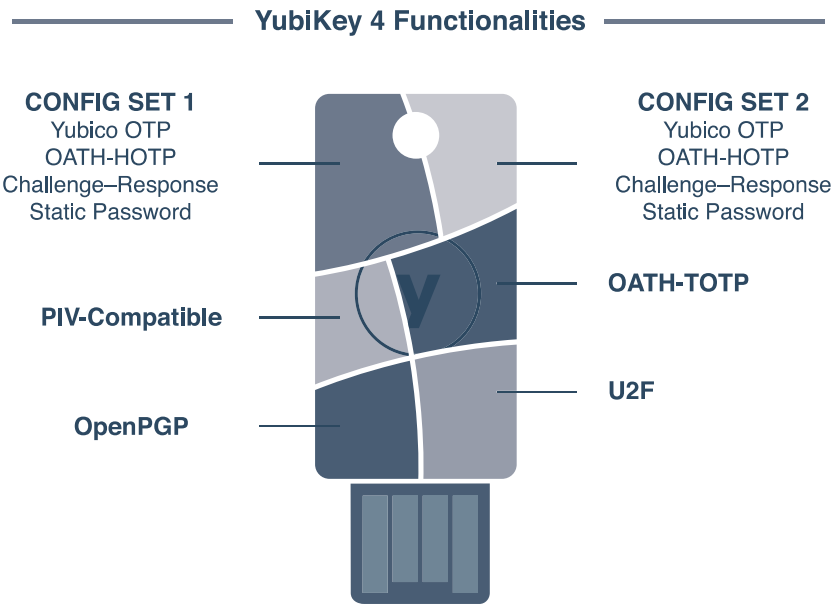
The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

## Contact Information

**Yubico Inc**
420 Florence Street, Suite 200
Palo Alto, CA 94301
USA
yubico.com/contact

Yubico has developed a multi-protocol authentication device, the YubiKey, which allows organizations to satisfy multiple authentication requirements. The three authentication functions the YubiKey provides allow the user to authenticate with a smart card, one-time password, and/or a FIDO authenticator, at the same time and on the same device. The YubiKey is a smart card that meets the highest level of assurance (LOA) requirements, based on NIST Electronic Authentication Guideline SP 800-63-2, which makes it an ideal candidate for deploying to both privileged and standard user accounts alike.

Additionally, using the same YubiKey as both a smart card and a one-time-password token allows organizations to bridge the gap between new and old authentication systems. Using the YubiKey as a one-time-password token and smart card enables organizations to centralize the provisioning of LOA 3 and LOA 4 authenticators onto a single device. The end result is that any organization deploying the YubiKey can solve their LOA 3/AAL2 challenges with OTP, a memorized secret, and their LOA 4/AAL3 challenges for users with smart card authentication. Lastly, the YubiKey is able to provide FIDO-based authentication to address the needs of future web-based authentication.




The YubiKey is a hardware token built using a mono-block design which is hermetically sealed in high quality resin. The YubiKey is exceedingly durable, and has received an IP67 class rating, as defined in international standard IEC 60529. The IP67 rating, and the fact the YubiKey can withstand 25 N·m of bending force, means the YubiKey easily resists common threats such as washing machines, spills, and weather. One of the core components in the YubiKey is a secure element that protects the key material against hardware-based attacks. The robust design of the electronic components and manufacturing process allows the YubiKey to easily meet the requirements FIPS 140-2 Level 3 for physical security. Yubico is currently listed in the FIPS 140-2 Modules In Process List.

Organizations and agencies issue PIV or PIV-I badges to their employees and contractors after successful background checks. The badges are used for physical access controls but many

organizations stop short of using them as a method for authentication to electronic systems. One barrier is the integration of PIV authentication with legacy applications. Since the YubiKey is able to authenticate with multiple protocols at the same time, the YubiKey is the ideal solution for integrating with a diverse set of electronic authentication methods while maintaining ease-of-use and relevant security controls.

The existing standard for electronic authentication NIST SP 800-63-2 lays out the current requirements for electronic authentication. A single identity assurance level (IAL) is directly mapped to a single authenticator assurance level (AAL). Implementing the highest level of authentication assurance, under this model, requires the highest level of identity proofing. Authentication assurance must match the identity assurance, which has had unintended consequences for overall system security.

To address this, NIST is currently working on a third version of the Electronic Authentication Guideline, SP 800-63-3, which simplifies the model for electronic authentication. The new model separates the assurance in the identity proofing processes from the assurance in the authentication event. This separation will make it easier to maintain security controls while providing citizen-facing services and in situations where temporary access is needed at the highest assurance level for an authentication mechanism.

| Level of Assurance (LOA) | Identity Assurance Level (IAL) | Authenticator Assurance Level (AAL) |
|---|---|---|
| 1 | 1 | 1, 2 or 3 |
| 2 | 1 or 2 | 2 or 3 |
| 3 | 1 or 2 | 2 or 3 |
| 4 | 1, 2 or 3 | 3 |

Under SP 800-63-3, organizations will have the flexibility to deploy YubiKey to provide the highest assurance levels for authentication while they mature their identity proofing processes.

Yubico believes that the YubiKey 4 provides the best user experience, best physical security protections, and most flexible deployment options for enterprises and organizations that comply with federal regulatory demands.