KeyScaler™ Platform Frequently Asked Questions

What is PKI Signature+?

PKI Signature+ is a new authentication method available in the KeyScaler platform that has been specifically designed to be used with low-power devices, where the patented Dynamic Device Key Generator ("DDKG") is not suitable. The solution utilizes asymmetric key signatures, coupled with policy-driven PKI based authentication and crypto key management enabling strong device identity and data privacy at IoT scale. This makes it easy for device makers to implement high assurance IoT Security for their applications.

How does PKI Signature+ work?

PKI Signature+ communicates with the KeyScaler server using WebSockets. WebSockets allow bi-directional communication between the client and the server without having to constantly re-establish the connection (e.g. sending headers, complete TLS handshake, etc.), thus reducing the amount of data and power required to complete an end-to-end function.

For enhanced security - all requests and responses between the device and KeyScaler platform are encrypted and signed by each party.

What are the key benefits of PKI Signature+?

- Developer-independent implementation, broader device support
- Low foot print, supports constrained devices
- Avoid cloning, impersonation
- Detect counterfeit devices

When is it appropriate to use PKI Signature+ and DDKG?

With the introduction of PKI Signature+, Device Authority now has two alternatives for device authentication technology. The table below provides use case scenario.

Use DA Agents with DDKG for	Use PKI Signature+ for
Linux-based devices, IoT gateways & cameras with 10+ MB of read-writable persistent storage. These can run DA Credential Manager or Crypto Agents	Embedded and resource-constrained devices that cannot run DA Agents Any IoT devices that need to make their own KeyScaler calls for security operations
Benefits	**Benefits**
Turnkey client-side solution Session-unique keys for authentication and derived crypto Owner-controlled security for IoT gateways & cameras Secure soft storage solution for devices without trusted storage for PKI credentials	Small executable footprint (xKB) Developer-independent implementation enabling broader device support

What is the ThingWorx Always-On Crypto Agent?

The Device Authority Crypto Agent for the ThingWorx Always-On protocol provides transparent, policy-based encryption for device applications connected to the PTC ThingWorx platform. This provides data security and privacy through transparent, policy-based encryption for device applications connected to ThingWorx.

How does KeyScaler 5.5 protect my IoT solution?

KeyScaler 5.5 provides strong device identity by assigning PKI keys to ensure only trusted devices are connected to applications. The Automated Password Management (APM) feature eliminates weak or default credential problems.

Does KeyScaler protect my company from DDoS?

Yes. Device identity and weak credentials are the primary methods in which attackers take control of the devices. KeyScaler protects devices from participating in DDoS attacks.

Does KeyScaler 5.5 work with any device?

Supported devices are listed in the AWS marketplace and in our Help Center.

We have extensive experience in adding new devices to our supported hardware list, and we are continually adding support for new devices. If your device is not currently listed in the support device list, please contact our support desk so that we can advise further: http://support.deviceauthority.com/

AWS Marketplace Link:
http://amzn.to/2uGefl4

DA Help Center Link:
https://deviceauthority.zendesk.com/hc/en-us/articles/115005376908

Can I have a demonstration of the new platform?

Yes. Please contact DA sales/support or register for a demonstration via this link:
http://info.deviceauthority.com/keyscaler_demo

How do I get started with KeyScaler 5.5?

If you'd like to purchase KeyScaler, then please contact us via http://info.deviceauthority.com/contact-form by email, phone or via the website form.

You can also purchase KeyScaler via the AWS Marketplace.
https://aws.amazon.com/marketplace/pp/B06XNYQPTZ

Do you offer a managed service, or do I manage the platform internally?

Today customers can stand up their own on premise solution or they can purchase a cloud-based solution from their channel partners. In the future, we may launch a Device Authority managed service.

How does KeyScaler 5.5 compare to other solutions in the market?

Device Authority offers a unique IoT security automation platform. Some vendors have a partially comparable solution or have repositioned their existing solution with similar messaging to KeyScaler. However, in our experience these solutions are not credible and we would strongly advise you to ask for comprehensive demonstrations of any product claiming to have the same functionality as KeyScaler, in addition to references and use cases. Please contact info@deviceauthority.com for a detailed competitive analysis.

Can I work with any certificate provider?

Device Authority currently supports issuing certificates from an internally created private PKI certificate authority service, and the public certificate authority, DigiCert. Integrations with Symantec and Comodo will be available in the future. Device Authority continues to expand its technology relationships with other Certificate Authorities.

How does KeyScaler prevent theft of certificates?

To prevent theft of certificates and unauthorized usage, the Device Authority agent stores the certificate and associated key pair in an encrypted state. The Agent will make decryption available only to authorized applications defined in the credential provisioning policy on the KeyScaler server.

Can I manage my own certificates internally?

Yes. KeyScaler supports issuing certificates from an internally created private PKI certificate authority service. KeyScaler provides the ability for customers to generate their own internal private root certificate authority and key, to enable provisioning of self-signed certificates to devices and the AWS IoT service. This means, as a customer, you can take control of your own security posture with reduced cost of ownership.

How does KeyScaler work with Amazon Web Services?

KeyScaler 5.5 has implemented an AWS IoT Service Connector using AWS SDK. This automates the certificate provisioning, revocation, as well as thing creation, and certificate assignment. AWS IoT customers are required to do all these things manually without this feature. KeyScaler 5.5 also has Internal Private PKI for easy and low cost Root CA for AWS IoT applications.

How do I purchase this from AWS?

KeyScaler is available in the AWS marketplace today:
https://aws.amazon.com/marketplace/pp/B06XNYQPTZ

What does the new Automated Password Management (APM) solution include?

- Automated user account password management to the KeyScaler platform
- Automatically set and manage local account passwords on devices, and rotate as per policy applied
- Restrict access to device passwords for privileged individuals only

Is there an audit trail for the APM solution?

Yes. A full audit of password changes is available to view in the KeyScaler control panel.

How many times can I rotate my passwords using APM?

The number of times is defined by the policy set. Passwords can be rotated as many times as required, without manual overhead.

DEVICE AUTHORITY
Trust for every Thing

sales@deviceauthority.com

www.deviceauthority.com

UK Head Office
2 Arlington Square,
Venture House,
Downshire Way,
Bracknell, RG12 1WA

North America Office
39300 Civic Center Drive,
Suite 180,
Fremont, CA 94538
USA