APP-XD

HIGH ASSURANCE CROSS DOMAIN

Technical Product Overview

#becrypt

APP-XD is a High-Assurance Cross Domain Solution (CDS) that was developed in collaboration with UK Government to provide flexible cost effective and highly secure connectivity across networks using API-based services.

#becrypt

Built with UK Government

APP-XD is based on the HiTMAN CDS architecture developed in collaboration with UK Government, as part of the Advanced Mobile Solutions programme. The HiTMAN architecture enables generic bi-directional CDS, a break from one-way or fixed use case appliances. The HiTMAN architecture is API-centric, enabling flexible and easy to use open standard interfaces for developer and operational teams.

HM Government

APP-XD is the first API-centric Cross Domain Solution, allowing organisations to interconnect critical services across different security domains, including high-threat domains, with bi-directional HTTP Rest APIs.

APP-XD

HIGH ASSURANCE CROSS DOMAIN

APP-XD is a High-Assurance Cross Domain Solution (CDS), providing secure connectivity for applications and services communicating across diverse and high risk networks.

APP-XD provides a high degree of assurance for the protection of applications within sensitive environments, such as critical national infrastructure systems, when accessed externally. APP-XD controls and validates what information can flow in and out of networks, with far great assurance than commercial Firewalls.

APP-XD is the first API-centric Cross Domain Solution, allowing organisations to interconnect critical services within different security domains, including high-threat domains, with bi-directional HTTP Rest APIs. Sample applications include:

Document validation

Strip harmful content and validate common document formats crossing network boundaries.

Secure file browsing

Secure release control of protected documents from high-side servers to secure low-side devices.

Management Infrastructure Protection

Isolate high-side management platforms from managed endpoints.

Bespoke Service Integration

3rd party developers can use an SDK to develop APP-XD compatible services to address an infinite range of high-side to low-side service integrations – all with a common and familiar DevOps oriented workflow.

Key Features

- Supports secure API integration across trust domains
- Bi-directional HTTP Rest support
- High Assurance architecture for military and critical systems
- Government (CAPS) and commercial variants available
- Avoids low-side data exposure through hardware-based decryption
- Simplifies multi-diode architectures to a single device
- Hardware based message validation
- Remote management for secure patching and audit
- High-performance (10GB) throughput and support for multi-device load balanced architectures
- Enables independent developer-friendly ecosystem, with software emulation support
- Avoids static CDS architectures to minimise through-life cost of ownership and dependencies
- Avoids data modification for support of Zero Trust Architectures.
- Single Appliance supports multiple simultaneous applications.

Security

APP-XD avoids the requirement to decrypt traffic on the gateway's 'low-side', allowing network traffic to be safely decrypted within the device FPGA (Field Programmable Gate Array).

Hardware-based encryption simplifies CDS architecures that have historically required multiple diodes, such as document validation and encrypted file import, achieving equivelent functionality with a single gateway.

Uniquely, APP-XD does not modify data once validated, avoiding data corruption for items such as digital certificates, and supporting Zero Trust Architectures across trust boundaries.

Management

APP-XD comes with remote management allowing the low-side and high-side and firmware components to be patched from a single management plane. This is achieved securely by ensuring that all communication between management and data plane over an HTTP interface are separately validated. Audit events may be exported to Syslog and compatible SIEM platforms.

Performance

APP-XD's high-performance platform supports 10GB throughput and as a web server based architecture, is compatible with load balancing for multi-device deployments to support scaling and resilience. The high performance architecture allows multiple applications to simultaneously execute on a single device.

Application development

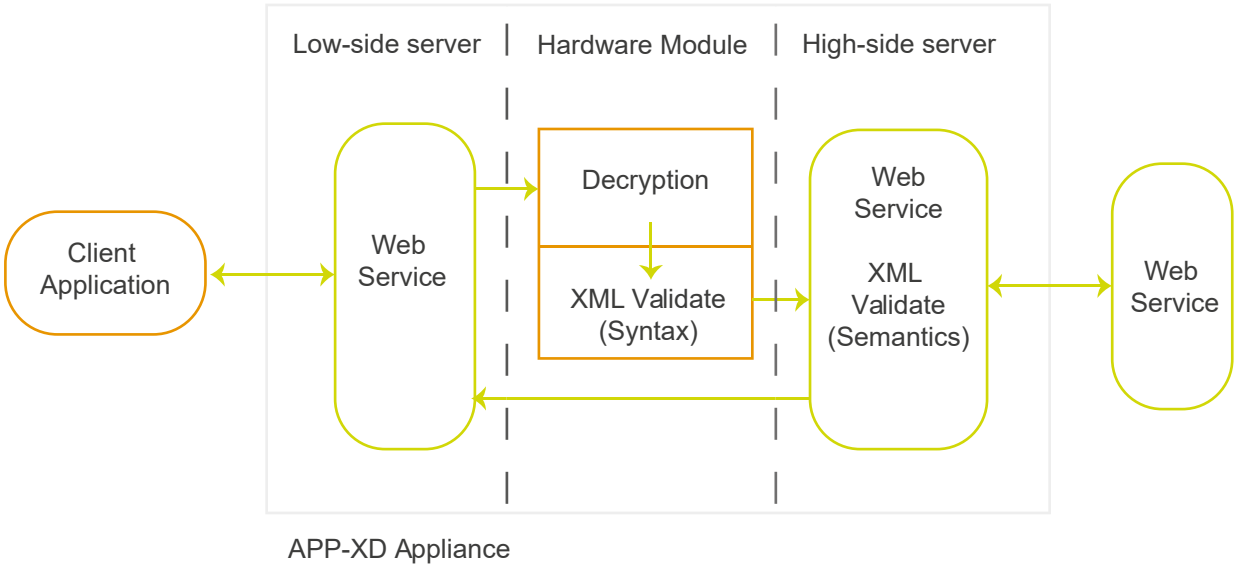
APP-XD is extensible, and designed to support a developer ecosystem. Becrypt provide an SDK and APP-XD software emulation to support rapid application development, and minimise the need for deep CDS domain experience for developer and DevOps teams.

Architecture

A High Assurance CDS requires to have clear separation between externally exposed components, and internal components which have connectivity to more protected core network systems and services. High Assurance standards require that:

- Import and export flows are separate;
- There is a hardware enforced one-way flow for import and export paths.
- There is a hardware enforced 'protocol break' to extract relevant information and use this to initiate a new transmission path.

This architecture protects high-side services from vulnerabilities throughout the network protocol stack, such as TCP/IP and SSL vulnerabilities that commercial firewalls are susceptible to. For APP-XD, a bidirectional hardware module forms the main security boundary point, sandwiched between a high-side and a low-side server-class processor – collectively forming a single APP-XD appliance.



The architecture allows a client in a less trusted security domain (low side) to make HTTP requests of web services from a server in a more trusted security domain (high side), and for the reverse. Client applications are either 'APP-XD-aware', and make use of an APP-XD library for gateway interaction, or communicate via an 'APP-XD-aware' low-side proxy server. APP-XD avoids low-side data aggregation, by allowing the client application to optionally encrypt messages that are decrypted within the APP-XD hardware module.

APP-XD messages are constructed by client applications using XML for message payloads. The first phase of data validation occurs within the APP-XD hardware module, to ensure that all messages are well-formed XML, and thereby preventing an XML parser exploit. This process is referred to as XML syntactic validation.

A second stage of data validation is concerned with validating that the well-formed XML makes sense to the application receiving it, referred to as semantic validation. Semantic validation ensures that the data is not malicious or dangerous in the context of the receiving application. Semantic validation rules take the form of XSD (XML Schema Definition files) defined by application developers. Optionally, data that cannot be validated, such as arbitrary binary data may be rendered inert within the high side through automated data wrapping.

APP-XD supports low-side and high-side service authentication, but also maintains data integrity through import and export pathways allowing digital identity management as required for Zero Trust Architectures.

APP-XD Development v Off-the-shelf

A key feature of APP-XD (and a driver for its initial government funding), is that anyone can write APP-XD-aware applications or services, allowing an ecosystem to evolve to address an infinite range of enterprise application requirements. Consumers of APP-XD may therefore either be solution developers, or consumers of pre-exiting solutions as outlined in the Applications section below. APP-XD applications range from the exchange of small, low-latency, interactive messages, to asynchronous transfers of large files, documents and emails with content validation. For solution developers, an Azure-hosted software implementation of APP-XD can be provided for development and integration testing, with a web-based training platform 'APP-XD School' for prospective developers.

Product variants

APP-XD Yellow

APP-XD Yellow leverages a High Grade NCSC CAPS Approved Hardware platform.

High Grade

APP-XD Black

APP-XD Black is a High Assurance solution, leveraging the same FPGA HiTMAN compliant architecture as the CAPS variant. Suitable for use up to SECRET.

High Assurance

APP-XD Red

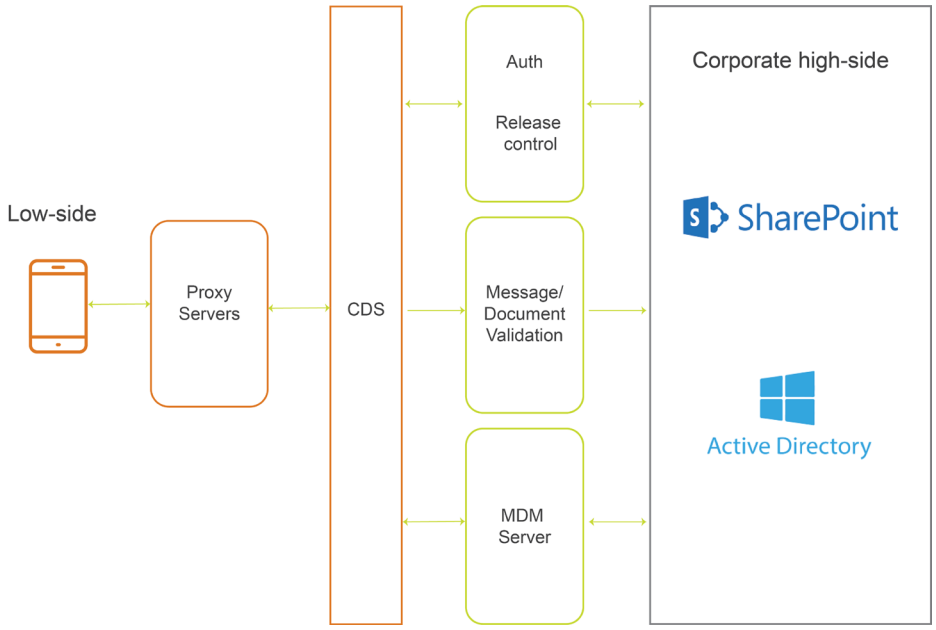
APP-XD Red is a software-based implementation of the HiTMAN architecture. Fully compatible with APP-XD hardware variants. Configurable as a web application Firewall (A WAF, but withouth the security properties of the hardware variants) APP-XD Red is extensively used for system development and test.

Software

Sample Applications

The diagram below provides an example of an existing application using APP-XD to control access to sensitive (high-side) documents. The capability outlined was developed in collaboration with UK Government to provide file-share connectivity between two or more trust domains, ensuring only documents authorised for release are accessible to authenticated users from managed devices.

In this example, an APP-XD compatible mobile application is able to retrieve documents from SharePoint or a fileshare, using the Gateway's encryption for low-side message protection. In this example, the device's security functionality is employed by the application to contain, encrypt and protect device data. User and device authentication protocols traverse and are validated by the APP-XD gateway. Additionally, the MDM platform used is CDS compatible, allowing the MDM server (and its high-risk contents) to reside on the high-side of the CDS. This is achieved by separating MDM messaging traffic and protocol handling between the MDM server, and a series of MDM proxy servers.



Simplified Secure File Browsing Architecture

Other sample applications Include:

Server Synchronisation Synchronising business services such as corporate calendars between high-side and low-side environments.

Structured Data Import With its plug-in architecture, APP-XD can validate any well-structured data using schema definition files for anything from geospatial to CAD file formats.

Syslog Ingest Development of bespoke and line of business client applications or proxy servers for secure API-based connectivity between trust domains.

Management across domains Enterprise platforms, such as virtualization technologies expose management functionality via an API accessible over an APP-XD gateway.

Custom Service Integration Development of bespoke and line of business client applications or proxy servers for secure API-based connectivity between trust domains.

Technical Specification

	APP-XD Yellow	App-XD Black
CAPS Approved Hardware*	Yes	No
HiTMAN Compliant Architecture	Yes	Yes
Decryption in hardware	Yes	Yes
XML Verification in hardware	Yes	Yes
Multiple applications per appliance	Yes	Yes
Data rate	10 Gbps	10 Gbps
Security enforcing functions	Hardware verification of data (FPGA Chip)	Hardware verification of data (FPGA card)
Operating temperature range	0 - 35 C	0 - 35 C
Dimensions	19", 1U	19" 2U half depth
Weights	20 Kg	26 Kg
Interfaces	HTTPS	HTTPS
Connectors	QSFP 10Gbps x 2, QSFP 1Gbps x2	QSFP x 4, 1GB, 10GB, 40GB, 100GB
Mains power supply	Dual Power Supply 110 - 240 VAC	Dual Power Supply 110 - 240 VAC
Cooling	Fan Assisted	Fan Assisted
Direction	Bi-directional & Uni-Direction*	Bi-directional & Uni-Direction*
Access to Appliance	Rear	Front
Structured HTTP traffic	Yes	Yes
Unstructured data	Quarantined	Quarantined
Automated patching	Yes	Yes
Integrated High/Low side management	Yes	Yes
Remote management	HTTPS Interface	HTTPS Interface
Availability	99.99%	99.99%

*Applies to underling hardware platform used for data transfer

#becrypt

Why Becrypt?

With a heritage of creating National Cyber Security Centre-certified products, Becrypt is a trusted provider of endpoint cybersecurity software solutions. Becrypt helps the most security conscious organisations to protect their customer, employee and intellectual property data. It has an established client base which includes governments (central and defence), wider public sector, critical national infrastructure organisations and SMEs.

As one of the early pioneers in device encryption software to today being first to market with a unique desktop operating system, Becrypt continues to bring innovation to endpoint cyber security technology. A recognised cyber security supplier to the UK government, Becrypt's software also meets other internationally accredited security standards. Through its extensive domain and technical expertise, Becrypt helps organisations optimise the use of new technologies and its HiTMAN platform delivers the security required for the modern age.

GET IN TOUCH

If you would like to find out more about HiTMAN, please contact us on:

0845 838 2080

or email us at:

info@becrypt.com