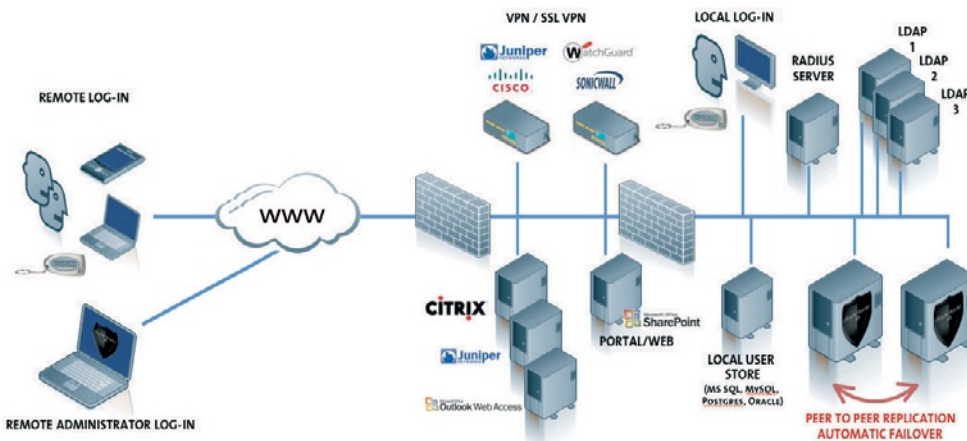


# BlackShield ID

## Architecture & Performance

BlackShield ID is a high performance, resilient, enterprise authentication server. It tightly integrates with your existing network components so that they are leveraged rather than duplicated. And by using a web services architecture it is able to make use of standard interfaces to ensure compatibility with a wide range of devices and applications. Security has been paramount in the design of the BlackShield architecture, assuring protection of data and reducing risk at every possible interface or data store.



Typical customer installation

### Small, Powerful, Scalable

Based on Microsoft .Net 2.0 framework (or higher), which is installed and running on all 2003/ 2008 servers by default, BlackShield ID is highly compact and efficient. Future versions of BlackShield will be developed on Mono so that they can be run on a variety of Operating Systems such as Unix, Linux and Mac OS.

This architecture not only delivers features that underpin its unrivalled performance and scalability, but it also ensures that BlackShield ID integrates with a wide variety of devices and applications to provide a seamless authentication infrastructure.

Leveraging the .NET framework, BlackShield ID runs inside IIS – which means that IIS is leveraged to manage all system resources in an efficient manner. BlackShield ID is an event driven web application and as such uses virtually no resources when idle.

BlackShield ID can support from 1 to millions of users off the shelf within a single server instance.

At under 30MB including the default database, it demands little overhead from system resources – allowing it to run on even low specification servers. BlackShield ID can also be run within virtualisation technology such as VMware.

### High performance

BlackShield ID is able to process hundreds of authentication requests per second in under 10MB of RAM on a low-specification server, and can reach a multiple of this on more powerful servers. In live customer environments, it has been shown to respond to a full LDAP lookup of 50,000 users in 2-3 seconds, and BlackShield ID is generally faster than a native LDAP look-up.

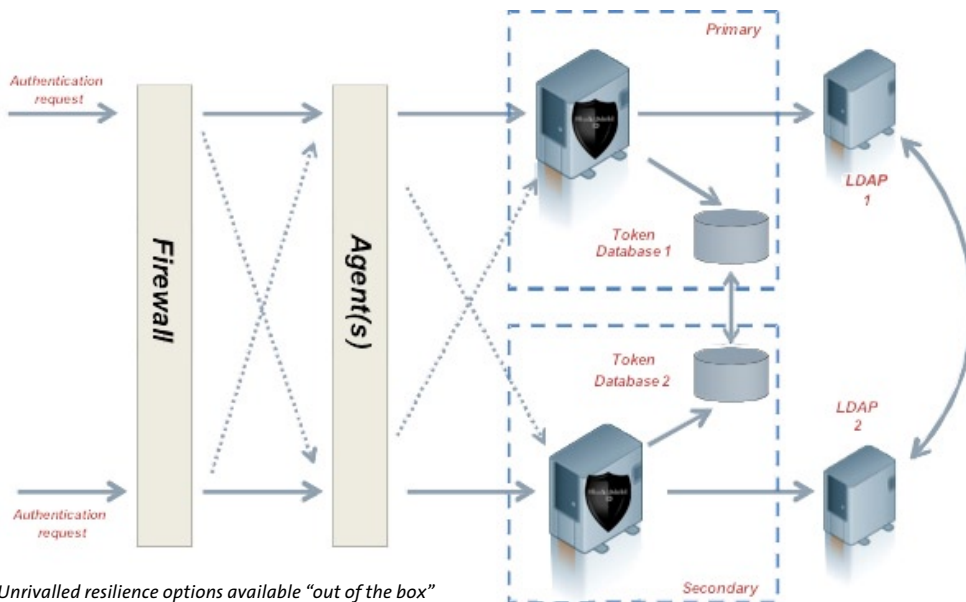
With automatic distribution of applications across multiple cores, BlackShield ID delivers superior performance. If it is installed on a dual or quad core processor, functions such as authentication and management are automatically distributed across the cores available. This also means that one activity is not impacted by another.



### Flexible integration with your existing network architecture

BlackShield ID has been designed to use, and integrate with, existing network components: from LDAPs to RADIUS servers to standard databases. The design philosophy was “less is more, simple is better”. Why duplicate user stores? Why install custom authentication agents if they are not needed? Why introduce new databases that require different backup and replication?

- Although every network is unique the concept remains the same: BlackShield ID will integrate tightly but flexibly with your existing network components.
- BlackShield ID is unique in its ability to connect to multiple LDAPs, but it doesn't interfere with them and it requires no schema changes. Further flexibility is provided by the ability to run a concurrent local user store alongside your LDAP connection.
- BlackShield ID supports standard Microsoft (and other) RADIUS servers, rather than requiring complex custom agents. Agents are used where RADIUS is not desirable.
- BlackShield ID supports multiple database choices so that a company's existing database standards, procedures and expertise can be used.



Unrivalled resilience options available "out of the box"

### Resilient architecture

BlackShield ID supports a secondary server as standard and at no extra cost, providing automated failover and industry-standard backup capabilities.

BlackShield ID is capable of operating in a multi-installation environment where more than one instance of BlackShield ID Pro is installed. To configure the failover between sites/servers, BlackShield ID automatically takes you through an install process as part of its installation "wizard".

All agents or RADIUS devices can be configured to authenticate to a secondary server should the primary fail assuring continuity of service.

Automatic LDAP failover is included within BlackShield as standard, allowing the server(s) to be connected to multiple LDAPs. BlackShield ID continuously monitors the availability of the LDAP and will automatically failover to the secondary LDAP server should it become unavailable.

The token database can either be based upon the in-built PostgreSQL database – that is automatically configured during the install process – or can be configured to use a standard database such as Oracle or MS-SQL. The standard high availability operating procedures recommended by the database vendor can then be used to ensure that the data is replicated between multiple servers ensuring an up-to-date image of the token database is always available.

A variety of database configurations and replication modes can be supported, including clustering, depending on the requirements for performance, availability and business continuity.

Continuity of service is also supported by the real-time monitoring and automatic systems reporting features which alert the Administrator to a variety of systems and performance issues such as low disk space or restart of the server. These alerts can be sent to any of the nominated operators via an email – ensuring immediate responses by support resources are possible.

### Secure Architecture

The architectural design of BlackShield ID is based on fundamental security principles to ensure that all data, communications links and interfaces are as secure as possible.

### Protecting data and links

All sensitive data is encrypted in the BlackShield database. In fact, each row in the database is encrypted using a unique key – as opposed to a single key used to encrypt the entire database. The database is also locked down and only the Administrator is able to move it – ensuring maximum security and peace of mind over the integrity of the data.

BlackShield ID uses the run time environment's in-built security functions to do the encryption so there are no export control restrictions unique to the solution. AES256 is used as the encryption standard throughout – which is about as secure as you can get!

All information sent from the agents or RADIUS devices to BlackShield ID are encrypted and the connection between BlackShield ID and the LDAP directory supports LDAPS/TLS, so all data transfer between the two entities is encrypted if LDAPS/TLS is enabled within the network. And of course all administrator connections for web-based management support SSL.

## BlackShield ID Architecture & Performance

### BlackShield ID System Requirements

**Operating System**  
Windows 2003 Server SP2  
Windows 2003 R2 Server SP2  
Windows 2008

**x86 Architecture**  
32-bit and 64-bit

**Web Server**  
IIS 6.0, IIS 7.0, .NET Framework 2.0,  
MSXML 6.0 SP1

**Processor**  
Pentium 4, 2.0 GHz+

**RAM**  
1 GB

**Disk**  
150 Mb for application, 2 kB / active token, 1 kB / authentication with full detailed logging enabled

### Network

TCP/IP Ports: 80, 443

**Authentication Protocols**  
RADIUS

### Supported RADIUS servers

Internet Authentication Service (IAS)  
Network Policy Server (NPS)  
Juniper Steel-Belted RADIUS 6.x

### Authentication Methods

2-factor one-time password  
BlackShield Static Password

### Password Protocols

PAP

### Supported Token Databases

MySQL 5+ (optional)  
MS SQL 2005 (optional)  
MS SQL 2008 (optional)  
Oracle 10g, 11g (optional)  
PostgreSQL 8.x

### CRYPTOCARD North America

340 March Road  
Suite 600  
Ottawa, Ontario  
K2K 2E4, Canada

Toll Free: 800-307-7042  
Tel: +1-613-599-2441  
Fax: +1-613-599-2442

### CRYPTOCARD Europe

Eden Park, Ham Green  
Bristol BS20 0EB,  
United Kingdom

Tel: +44 870 7077 700  
Fax: +44 870 7077 711

E-mail: [info@cryptocard.com](mailto:info@cryptocard.com)  
[www.cryptocard.com](http://www.cryptocard.com)