



BlackShield ID

Total authentication, made simple



Greatly reduced total cost of ownership



Best-in-class security



Simpler, quicker system administration



Straightforward, rapid deployment and integration



Industry-leading performance



Unrivalled end-user experience

BlackShield ID is the new authentication server from CRYPTOCard combining a broad feature set that delivers low total cost of ownership. Use of leading edge technology simplifies integration and administration while delivering unrivalled performance. Real-time reporting, a comprehensive security policy, compliance and audit capabilities set it alone in the two-factor authentication market.



Greatly reduced total cost of ownership



An all-inclusive enterprise-wide approach with no costly 'extra' components, the most robust non-expiring tokens in the industry, automation and provisioning tools, and the lowest administrative requirements.

Put simply, BlackShield ID provides the best TCO on the market. Savings are made in a number of key areas:

- Extremely rugged, non-expiring tokens
- A complete and resilient software suite with no costly add-ons
- A major reduction in the time and resources required to manage and administer the solution.

Peace of mind through longevity

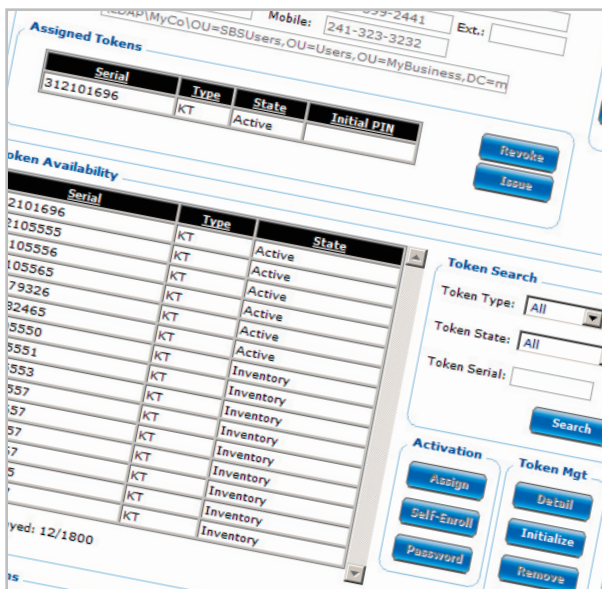
CRYPTOCARD's hardware tokens are renowned in the market for their ruggedness and durability. More importantly, no expiration is imposed on their use, leading to reduced token purchase costs and reduced logistic and deployment costs (imagine rolling tokens out to users once every seven years rather than every two to three years).

All-inclusive software suite

BlackShield ID includes an all-in-one solution so that your organisation has no need to invest in any additional components. The suite includes:

- Authentication agents (for example Citrix, SharePoint and domain log-in)
- Token deployment tools (self-enrolment and bulk enrolment)
- A replica server.

Additionally, there is no need to purchase or license a separate server for each LDAP – BlackShield ID can authenticate users from multiple LDAPs.



BlackShield ID delivers a further reduction in TCO through reduced costs and increased efficiencies:

- *Deployment* – through the automation of provisioning, Bulk enrolment and self-enrolment
- *Administration* – with real-time views, alerts and comprehensive reporting
- *Management* – process and workflow automation coupled with easy integration
- *Help desk* – user self service portal and real time system views for rapid ticket resolution

Activation and management at the click of a button reduces management costs

“If any organisation is looking for an easy way to escape expensive licensing models, I would not hesitate in recommending CRYPTOCARD.”

Stephen DelVecchio, i2



Best-in-class security



The flexibility to customise BlackShield ID to support your security policies now and as they change, automatic alerts if security thresholds are exceeded, and comprehensive logging and reporting features; all adding up to unrivalled compliance and audit capabilities.

BlackShield ID makes it easy for businesses to implement their authentication security policy and address matters of regulatory compliance and audit requirements. Administrators have a wide choice of options across a variety of key policy areas.

Security policy support

BlackShield ID is fully customisable to support a company's security policy, rather than dictating it:

- Flexible PIN and one-time password length and complexity (for example a six digit numeric password or an eight character complex password incorporating numbers, letters and punctuation)
- Lock and unlock policies, plus alerts for dealing with account abuse and hacking detection
- Time of day and week access controls
- Parameters for out-of-sync protection
- Temporary access controls for handling lost or stolen tokens.

CRYPTOCard offers its clients the ability to initialise their own tokens, so that the unique token seed used to generate the one time password is not shared with an external party.

Compliance and audit

Administrators can be proactively alerted to suspicious activity, allowing action to be taken immediately and thereby further strengthening compliance.

All authentication and operator activity is recorded and can be easily accessed by built-in reporting or via external SQL tools. Token activity history is never lost, regardless of re-initialisation, reassignment or deletion of tokens, providing a permanent and complete audit trail. Logging output can be sent to the event viewer, making it easy to capture and analyse the data.

Secure user deployment

Self-enrolment offers a highly secure deployment option that ensures secure activation of the token by only the intended recipient – irrespective of third party involvement in the deployment process – removing security concerns about insecure token and PIN delivery. There's no need to manually send a PIN and instructions via e-mail, or even to write them on the box in which the token is being delivered! Tokens aren't left 'hanging' and unused until the self-enrolment process is completed or the token is disabled.

The screenshot displays the CRYPTOCard administration interface. At the top, there are navigation tabs: NAPSHOT, SECURED USERS, ASSIGNMENT, CONTAINERS, and REPORTS. Below these, there's a section for 'Synchronizati' with options for 'Inner OTP syn' and 'Outer OTP syn'. The main area is titled 'Token Templates' and includes an 'Edit' button. Underneath, there are several policy configuration sections: 'Authentication Thresholds' with fields for 'Account Lock threshold' (set to 3) and 'Account Lock duration' (set to 15 Minutes), and checkboxes for 'Alert Operator on Account L'. The 'Server-side PIN Policy' section includes checkboxes for 'Change PIN on first use required' (checked) and 'Force Random PINs', along with fields for 'Minimum Length' (3), 'Maximum Length' (8), and 'Random PIN Length' (4). The 'Temporary Password Policy' section has checkboxes for 'Temporary password Allowed' (checked) and 'Change Password on first use required' (checked), with fields for 'Minimum Length' (8), 'Maximum Length' (16), and 'Lifetimes' (1 Hour).

Choose your security policy from a wide choice of parameters



Simpler, quicker system administration



BlackShield ID's real-time reporting and management tools allow IT professionals to concentrate on core business. The user self-service portal and process automation features reduce the burden on help desks, allowing organisations to realise significant efficiency savings.

BlackShield ID allows IT professionals to concentrate on core business. By reducing the instances of account unlock or token reset, organisations are able to realise significant efficiency savings.

Monitoring system log files or exporting data to a separate reporting application is no longer necessary. Real-time information is delivered proactively so that issues can be dealt with instantly.

Real time system activity views

BlackShield ID incorporates real-time views of system activity, facilitating a massive reduction in help desk operatives' time to resolve calls. Whether in the dedicated snapshot tab, or within the screens of the secured users tab, all the relevant data is displayed in real time, from viewing the last 100 authentications to analysing the results of PIN change attempts.

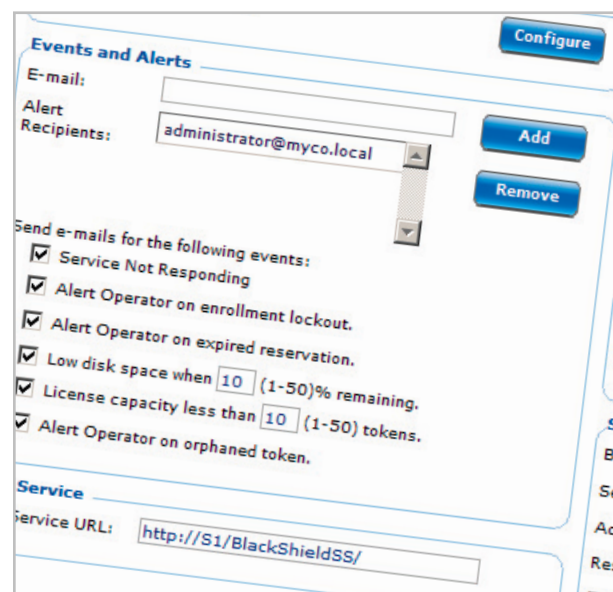
Management by exception

A key attribute of BlackShield ID is that the administrator is no longer required to monitor the system. Alerts can be set to report if security policy thresholds or system operating thresholds are exceeded – such as locked accounts, unauthorised authentication attempts, failed management log-ins and low disk space. This functionality also acts as a 'hacker alert' as suspicious activity will be notified. It can even be utilised as a pre-emptive 'user problem alert' as user log-in problems can also drive alerts.

Tab-based browser

BlackShield ID boasts an intuitive browser-based user interface which has been designed to optimise administration by grouping related tasks within individual tabs. For example, the Secured Users tab groups typical helpdesk operations. Within one tab, the administrator can set PINs, assign a temporary password, reassign a token, and execute a host other typical administrative tasks – all within two mouse clicks.

The tab-based layout also forms the basis of operator permissions which improve system security by ensuring that operators are only able to perform tasks appropriate to their role, by limiting which tabs are visible for the individual role. The administrator can also add a note against any action, so that the full history is recorded.



Key system parameters can trigger alerts, improving the efficiency and timeliness of your helpdesk support



Simpler, quicker system administration



Workflow and provisioning automation

An administrator can choose to use the simple administration browser for basic user and token management. They can also perform the same tasks by running a command line that will execute these tasks for thousands of users at the same time.

The administrator can also decide to automate a wide variety of processes and tasks – such as token deployment, end user self enrolment or account lock and unlock. Combined with the management-by-exception functionality, the level of administrator time required is massively reduced.

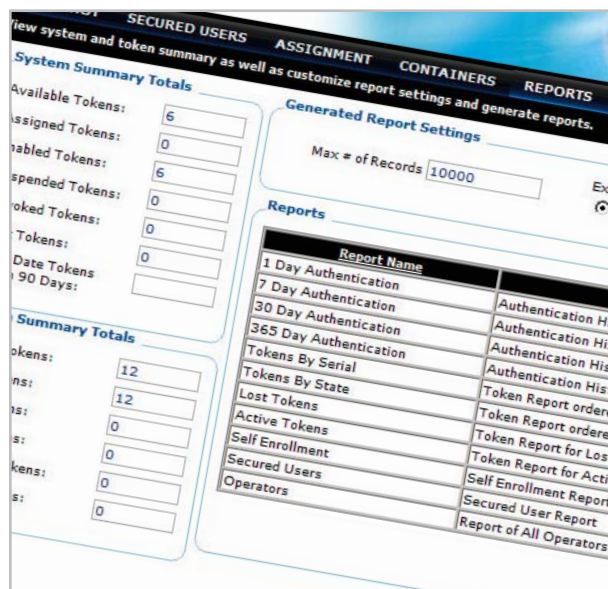
Dependent upon criteria set up by the administrator, users can self-enrol – a process whereby the user enables his token when it is received. This removes the need to manually pass PIN information and registration details to the user, or manually check if the token has been received and activated.

BlackShield takes care of token assignment, inventory management, user notification and administrative alerts if the process is not completed as expected. Additionally, BlackShield ID is easily integrated with external workflow and provisioning applications to automate provisioning.

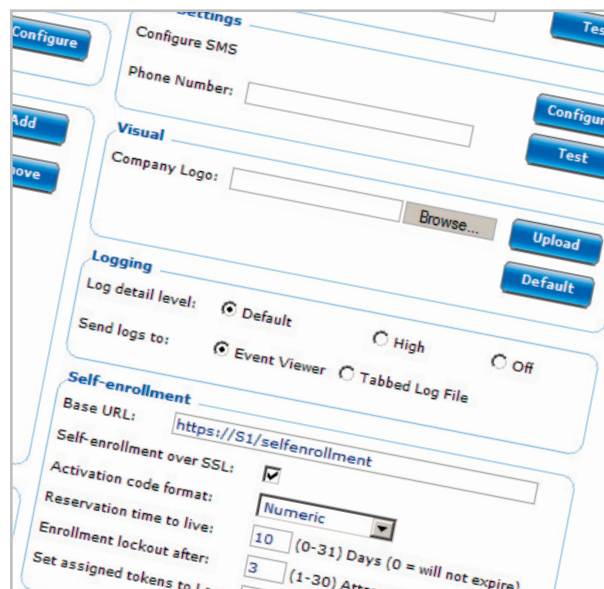
User self-service portal

BlackShield ID features a fully-customisable user self-service portal where a user can perform simple functions such as PIN changes and requests for on-demand tokens, further reducing helpdesk overhead.

Even better, if tokens need re-synchronising, for example when the button on the token is accidentally pushed repeatedly, BlackShield ID automatically steps-in and solves the synchronisation problem at user log-in, avoiding a helpdesk call.



Empower your management decisions with a broad array of simply generated reports



Provisioning made easy using BlackShield ID's self-enrolment functionality



Straightforward, rapid deployment and integration



All agents for network and application integration are included out of the box, including integration with multiple concurrent LDAPs.

Applications and networks

Authentication agents allow organisations to secure applications and devices such as Web applications, Citrix, OWA or VPNs. The agent is typically installed on the appropriate server or application and interacts with BlackShield ID to deliver secured access.

BlackShield ID includes a wide range of agents at no additional cost.

Organisations can use Access Control Lists to specify which agent can talk to BlackShield ID. All traffic between agents and the server is encrypted.

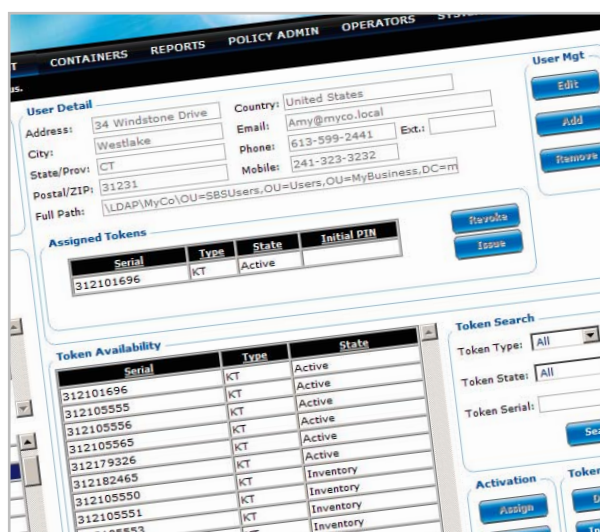
User directories

BlackShield ID tightly integrates with existing user directories, such as LDAP, as well as offering an internal database to support users that do not, or should not, exist in LDAP. Uniquely, it can support multiple LDAPs within a single server instance, rather than requiring a separate server for every LDAP, giving immense flexibility and the most cost-effective network architecture.

No schema changes, synchronisations or user imports are required for LDAP integration. A real-time link ensures BlackShield ID always reflects the current LDAP data. In addition, BlackShield ID's unique LDAP PreAuth functionality allows administrators to use a user's existing LDAP attributes to control their access. For example, group membership parameters in LDAP can determine which access points a user can authenticate to.

Databases

Many organisations have established corporate standards for databases. BlackShield ID allows substitution of the default database included with BlackShield ID, with Oracle, Microsoft SQL, MySQL and Postgres.



Fast and secure import of user details from LDAP



RADIUS devices are supported via BlackShield ID agents located on RADIUS servers such as:

- Network Policy Server (NPS)
- Internet Authentication Server (IAS)
- Juniper Steel Belted RADIUS

Additional agents include:

- Outlook Web Access (OWA)
- SharePoint, Remote Web Workplace (RWW)
- Citrix Web Interface/XenServer
- Log-in Agent for Windows Domain Logon
- Log-in Agent for Windows Terminal Server
- Agent for IIS Virtual Web Sites
- Internet Security and Acceleration Server (ISA)



Industry-leading performance



BlackShield ID has a highly secure and resilient architecture. It executes hundreds of authentications a second and scales to support millions of users.

With virtually no demand on system resources, BlackShield ID can process in excess of 100 authentication requests per second in under 10Mb of RAM on a low-specification server, and can reach multiples of this on more powerful servers. It has been shown to respond to a full LDAP lookup of 50,000 users in 2-3 seconds, and is generally faster than a native LDAP look-up. BlackShield ID automatically distributes tasks across multiple processing cores, if they exist, assuring fantastic performance even when there are high levels of administrative activity running concurrently.

BlackShield ID provides automated failover and industry-standard backup, supported by proactive monitoring which alerts the administrator to performance issues, such as low disk space or server restart. It also supports high availability across all system components, for example, redundancy and failover for both LDAP and internal database user stores.

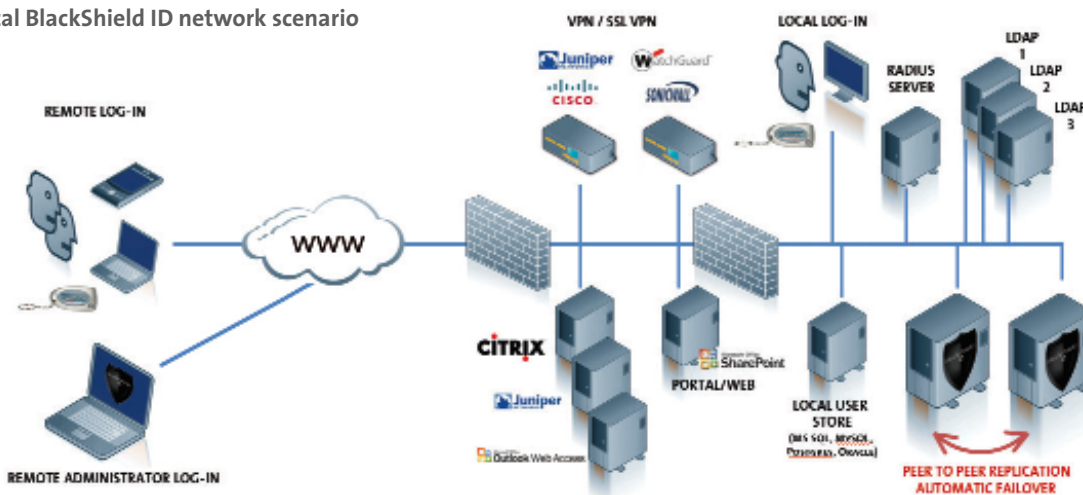
BlackShield ID is a Web services-based application. It has been written on the Microsoft .NET and Mono development platforms to ensure cross-platform compatibility and superior performance.

BlackShield ID is a highly secure application, with features that include:

- All sensitive data is encrypted in the database, even using a unique key for each row
- The database cannot be copied or moved to another machine without administrative privileges and access to an externally held cipher key
- Communication between system components (such as LDAP, agents and administration sessions) and BlackShield ID server are encrypted
- No passwords are stored in the clear anywhere in the system
- Remote management sessions require token authentication.

BlackShield ID installs on any Microsoft 2003/2008 server, 32 or 64 bit. Additionally, because BlackShield ID is a Web services application, it installs in IIS, consuming minimal system resources whilst delivering exceptional throughput and tight integration with other Microsoft server components, such as IAS/NPS, Active Directory and SQL Server. Client software for operators and administrators is not required and BlackShield ID can be managed from any location with a browser and Internet access.

A typical BlackShield ID network scenario



Unrivalled end-user experience



The huge range of tokens available make it easier to choose the right token for the right user, and unique award-winning token features make for an unsurpassed user experience.

The award-winning non-expiring CRYPTOCard tokens used by BlackShield ID are the most robust available and are supported by industry-leading warranties.

Token range

- **CRYPTOCard's robust hardware tokens** offer more configuration options and have the most durable steel casing available on the market.
- **Multi-platform software tokens** can be used on laptops, mobile devices (such as PDAs, BlackBerrys, Smartphones and mobile phones) as well as some smart cards and USB devices. CRYPTOCard's "One PIN and You're In" feature delivers unrivalled usability
- **On demand OTPs** provide a token code via an SMS message to a mobile phone. CRYPTOCard's "SMS-Now" solution ensures that the user always has an OTP, resolving issues of no network coverage and forgotten phones without help desk intervention.
- **USB stick and smart card tokens** allow for easy integration with other security solutions that require digital certificates – such as disc encryption solutions – or with physical security systems, such as door access systems or identity photocard.

- **Other hybrid tokens**, such as the CD-1, offer credit card sized OTP devices that can also be used for door access and as identity cards, and can even be integrated within standard debit or credit cards for use in Web and telephone banking authentication.
- **OATH-compliant tokens** from any manufacturer are supported, giving even further choice.

Managing your assets

BlackShield ID token lifecycle management ensures that maximum use is made of all tokens and allows the administrator to easily report on their asset base. Through the concept of token 'states' (inventory, assigned, active, lost and so forth) which reflect the lifecycle of the token, tasks can be automated and administrators alerted.

For example, if a self-enrolment process hasn't been completed, BlackShield ID will update the token state and alert the administrator. Compare this with traditional systems where the administrator must run reports to determine which users have activated their token and follow the exercise with manually identification and re-provisioning of tokens.

BlackShield ID offers a wide variety of token formats to satisfy all user scenarios



- KT-1 (key chain stainless steel token)
- KT-2 (key chain hard plastic token)
- KT-3 (key chain token with HID)



- RB-1 (PIN pad token)



- CD-1 (smart card token)



- SC-1 (smart card token)



- UB-3 (USB style token)



- ST-1 (software token)



- ST-1 (Blackberry/PDA software token)



- SMS token (mobile phone token)

CRYPTOCard


CastleForce
IT SECURITY
CryptoCard Certified Partner

CRYPTOCard

Tel North: 0151 2031400 Tel South: 0118 9071600
Email: Info@castleforce.com Web: www.castleforce.com

