

BlackShield ICE: Secure Remote Access Prepare for the unexpected

Business disruptions come in many forms: swine flu, bird flu, snow days, floods and transport strikes to name a few. All of these create situations where staff suddenly find themselves unable to get to work, and if you haven't prepared for additional secure remote logins, this in turn has a negative impact on business productivity and therefore revenue.



In Case of Emergency (ICE) planning is essential if your business is to avoid significant disruption and often involves allowing people to work from home. To achieve this, you will not only need to increase users accessing your network remotely at a moment's notice but also ensure access to the network is secure.

The BlackShield ICE solution helps reduce the security risk during a business disruption by allowing staff to log in using two-factor authentication rather than passwords which could leave your network open to hackers or ID thieves.

Why BlackShield ICE is Cool

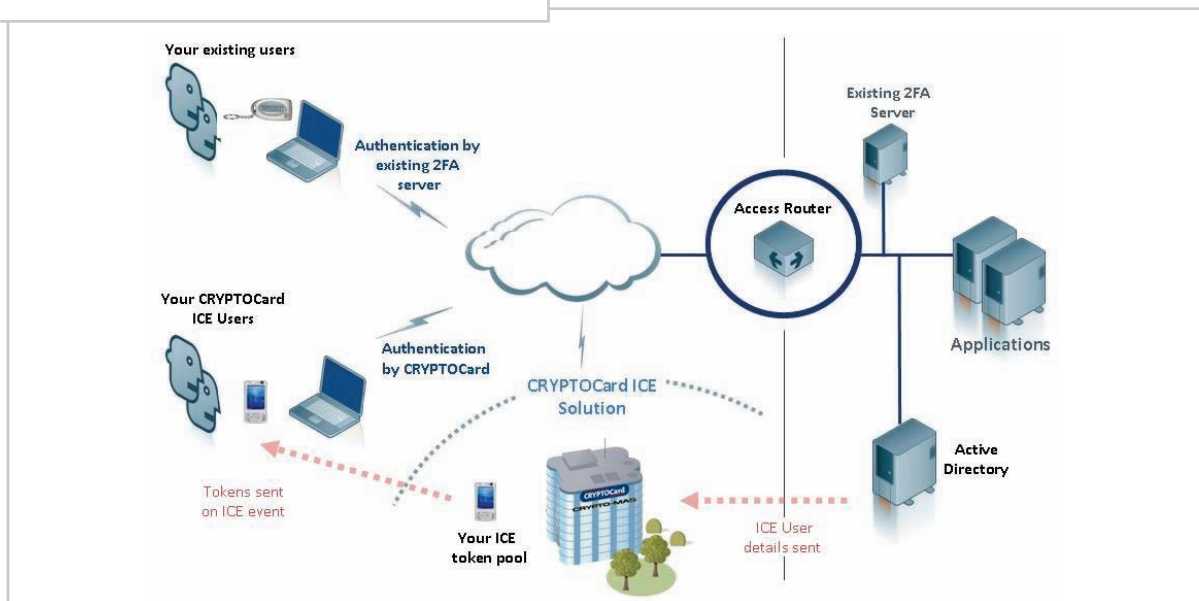
- No minimum number of active users required
- Works within an existing 2FA network (even non-CRYPTOCard!)
- No big upfront fees to pay
- Tokens always at hand for immediate use
- Can scale from 10 to 1,000,000 tokens
- Software or SMS token formats available

ICE Benefits

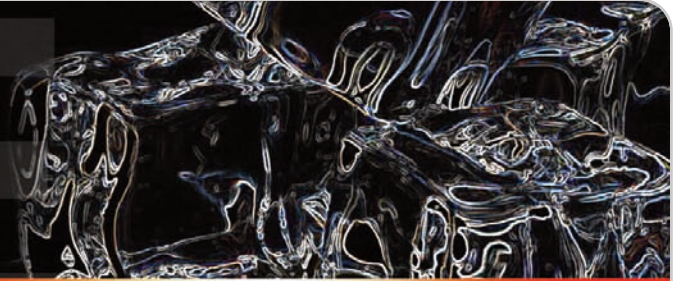
- You pay a small fee to purchase ICE tokens
- The tokens are made available to you immediately but are frozen until you need them
- When you need your tokens you can use a simple portal to send them to users – this happens within seconds

How ICE Works

- Define how many ICE tokens you want for your ICE users – there is no minimum number of active users required
- Purchase ICE tokens for a nominal per-user fee on a one-year support plan
- Provision users with ICE tokens
- Authenticate ICE tokens with users
- In Case of Emergency, IT simply clicks a button to activate
- The tokens are active for a minimum of 6 weeks, after which, they can be refrozen



ICE



ICE Roll Out & Activation

- ICE software and/or SMS tokens are purchased and distributed to the customer
- Tokens are distributed by IT to ICE users via an email (for soft token users) or text (for SMS users)
- ICE users are directed to the CRYPTOCard self-enrolment site
- Once on the CRYPTOCard self-enrolment site, they will follow the PIN and one time password process to activate their token
- Following testing, the ICE tokens sit 'frozen' within the BlackShield ID solution until they are required
- To activate ICE tokens, IT click a button to instantly 'defrost' the ICE tokens
- CRYPTOCard activate the tokens within minutes
- After the 6 week ICE period, you can choose to refreeze your tokens, or keep them active
- You may wish to keep some ICE tokens active but refreeze others, we can accommodate any requirements for additional permanent users from the ICE pool

ICE Drill

ICE tokens come with a seven day test license, enabling you to roll-out tokens to users for registration and live use. By testing the service in advance of an ICE situation, you can be comfortable knowing your users are familiar with the enrollment and login process, so they can be up and running as quickly as possible in an ICE situation.

About BlackShield ID

BlackShield ID is a web services based strong authentication, token provisioning and management application that enables organisations to efficiently and effectively protect against unauthorized logons resulting from shared, recycled, stolen or hacked static passwords.

BlackShield ID works on Microsoft 2003/2008 and is tightly integrated with Active Directory, ISA, IAS/NPS, IIS, OWA, SharePoint and SQL server and protects Windows network logon, Citrix, VPNs and WLANs, email, intranets and extranets, web servers and products from hundreds of technology vendors.

About CRYPTOCard

Twenty-years of technical achievements have won CRYPTOCard the trust of thousands of organisations in over 70 countries. CRYPTOCard's solutions reduce the risks associated with remote access and web-based processes through strong password security and increased compliance, at a price all businesses can afford.

The only company to offer authentication in server-based, managed service and build-it-yourself options, CRYPTOCard provides the most flexible solutions on the market for matching customer's password security policies.

“As a managed service provider, we have a responsibility to ensure we’re delivering business-grade services that optimise and safeguard our customers’ business operations. With significant growth in remote access and collaborative applications, identity and access management is now fundamental to enterprise security.”

Stephen Benyon, Managing Director, ntl:Telewest Business



CRYPTOCard Europe

Eden Park
Ham Green, Bristol
BS20 OEB
UK

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

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

info@cryptocard.com www.cryptocard.com

