ADSS GrIDsure Server

- Advanced one-time password services
- For web-based user authentication
- For application-based user authentication
- For transaction authorisation and digital signing

Identity Management is broad term covering corporate identity, role management, multi-system single sign-on and password synchronisation. Within this broad arena, there is much debate about how best to strongly authenticate users.

Financial institutions in particular have adopted new approaches that use multiple password plus questions and answers. However, end users do not find it easy to remember these, which often results in them being written down, immediately compromising the security benefits and increasing the risk of fraud.

All organisations are facing a variety of pressures to provide enhanced security for access to data, provide better internal controls, accountability, traceability and auditing.

Where users are not provided with hardware tokens to authenticate themselves and digital certificates are not available for client-server SSL authentication then one time passwords are a very good of strengthening security.

GrIDsure® (www.gridsure.com) is a new high-security identity authentication methodology that makes it easy to deploy and use strong authentication for today's typical users.

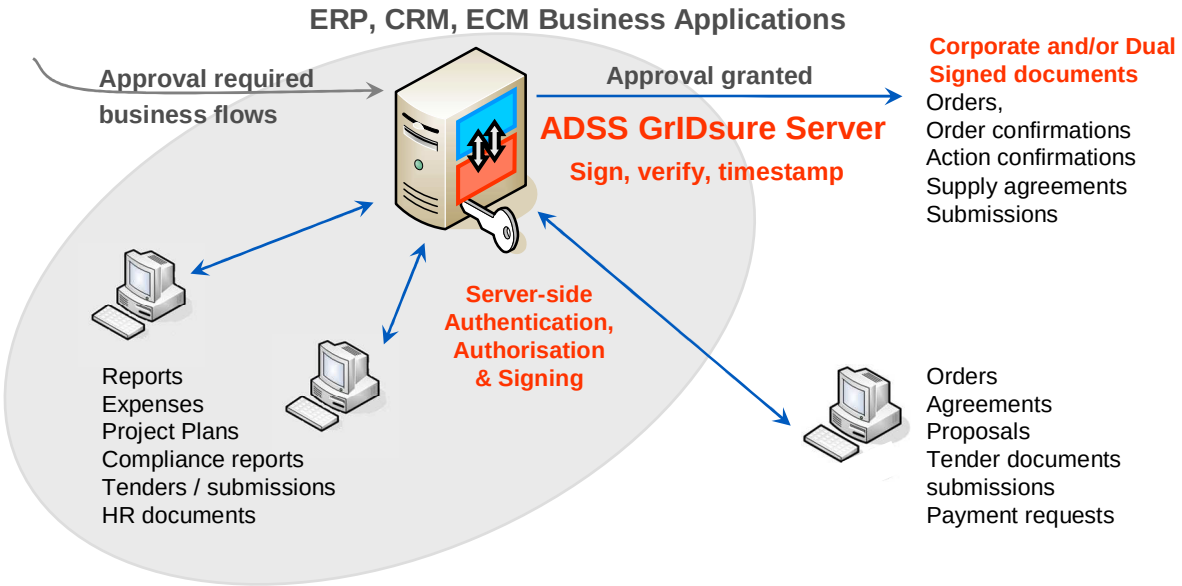
Ascertia has licensed this for use within the ADSS GrIDsure Server with a particular focus on both strong authentication and digital signature authorisation.

The core of GrIDsure's methodology is one of 'sequential pattern recognition' of cells on a grid. A pattern of cells is selected from a registration grid and stored securely within the ADSS Server. At any future time the user can be challenged with a grid containing randomly generated numbers and now simply selects those numbers from the grid that match with the pattern they registered. ADSS GrIDsure Server determines if the user is successfully authenticated and one server can enable multiple applications.

Once logged into the business applications the users can now also be challenged quickly and easily to confirm key transactions, e.g. confirming new payment beneficiary details, share purchases or sales, purchase orders, and any type of document approval, even on a mobile device!

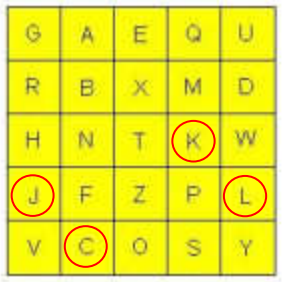
ADSS GrIDsure Server uses this authorisation to digitally sign the transactional data to create legal weight undeniable evidence to reduce business risks.

A Business Workflow with authentication, authorisation and signing services

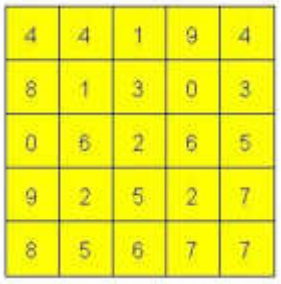


Strong user authentication, user authorisation and digital signature creation

User Registration: The user registers a 'Personal Identification Pattern' (PIP) with the ADSS GrIDsure Server. The grid can be any size or shape; however a 5x5 grid gives a good balance between ease of use and security in most situations The PIP can be 4 cells (like a PIN) and offers 390,000 one time password variations! 5 digits provides almost 10 million variations. In the example JCKL has been selected. At registration time ADSS GrIDsure Server also generates a key and certificate for the user so that they can sign data simply by authorising the signing action that the business application requests.



In normal use: The user is presented with a challenge grid populated with random numbers (they could be letters or symbols). The user enters the numbers representing their PIP sequence. Looking at the grid on the right the one-time password would be 9567. Next time of course the numbers will change and a different one-time password is thus created. It's that easy!



This password value is keyed into the business application and then checked with ADSS GrIDsure Server. The application doesn't need to generate grids or hold the PIP data – ADSS GrIDsure Server does all this and returns true or false. If a signing request is received then the ADSS Server checks the password response to the signing authorisation challenge is correct and then applies the signature as requested.

GrIDsure®

The following table show the multiple different ways in which ADSS Server can be integrated within a business workflow environment to suit existing systems and technologies and the user authentication and signing authorisation options that exist.

Signing Capabilities

- Sign various document / data formats
  - PDF, XML, File, Form (PKCS#7) and S/MIME
- Sign using various format options
  - Embedded – e.g. PDF, XML
  - Wrapping – e.g. PKCS#7 / CMS / XML)
  - Detached (XML, PKCS#7, CMS)
  - Plus timestamp information (ETSI / PDF)
  - Plus validation status information (ETSI / PDF)
- Notary / archive / evidence archive
  - Using RFC3161 timestamps
  - Using SHA-2 hash and long-length RSA keys
- For use with any internal or external document
  - Use Corporate server signatures
  - User individual client-side signatures via GoSign

ADSS Server Integration Options

- ADSS Server Web Services
  - via XML/SOAP messaging
  - via a provided high level .NET API
  - via a provided high level Java API
- Using ADSS GoSign
  - Within a web-browser (GoSign Applet)
  - Within a desktop .NET app (GoSign .NET)
  - Within a desktop Java app (GoSign Java)
- Using ADSS Server Automated Batch Mode
  - For one or more watched folders
- Using ADSS Gateway for confidentiality
  - to extract signatures from documents
- Using the Secure eMail Server
  - to handle emails and/or attachments

With so many options Ascertia and its local delivery partners can help you to define the best options to meet the various business, legislative and regulatory needs and reduce the risks and costs involved in user authentication, authorising and signing business documents. The multiple capabilities of the ADSS GrIDsure Server can be used to solve today's needs and also offer tremendous investment protection to meet the changing needs of tomorrow.

ADSS GrIDsure Server Standards Compliance:

Signature generation:	CMS/PKCS#7, standard PDF signatures. XML DSig and ETSI CAdES, XAdES long-term signatures
Time stamping:	TSP (RFC3161)
HSM Support:	Any PKCS#11 compliant HSM, e.g. SafeNet, nCipher, others
Operating Systems:	Windows 2003 Server, Solaris 10 (Sparc and x86), CentOS, other Linux on demand
Databases:	SQL Server 2000/ 2005, Oracle 10g, PostgreSQL, others on demand
Interfaces:	XML/SOAP messaging (including over SSL/TLS), HTTP(s) interface for administrators

GrIDsure and the GrIDsure logo(s), are registered trademarks of GridlockTS Limited

Ascertia Limited
Web: www.ascertia.com
Email: info@ascertia.com
Tel: +44 1256 895416 US: +1 508 283 1890
40 Occam Road, Guildford, Surrey, GU2 7YG, UK
© Copyright Ascertia Limited 2009. All Rights Reserved, E&OE

Signed By: Rod Crook
Reason: I approve this document
26/08/2009 12:20:33 GMT +01:00