Enabling Strong User Authentication and Online Document Signing Services

The Problem

One of the big issues for retail e-commerce web-sites is how best to maximise usability and security. For businesses that offer higher value products and services, non-completed transactions, fake requests and fraud are a substantial issue. Security needs to be good but non-intrusive. The user experience must be good enough to maximise order completions, but security needs to be effective enough to stop the reputation damage that can follow from poor choices. Consumer confidence is hard to build and very easy to destroy. The press are always looking for a good story about information losses, users being defrauded and hacker successes.

Enhanced Solutions

To try to strengthen the traditional username and password access to a web-site a number of complex registration schemes have been created by various organisations. Multiple question and answers, password letter selection and other approaches can be quite cumbersome and weak, e.g. some banking questions and answers are also asked on simple social web-sites. The key to success is to make the authentication process difficult enough to be secure and yet easy enough for the average person to use with a high degree of success.

One time passwords are good because the password continuously changes so there is little to be gained from password capture. These have traditionally required a hand-held device that generates the one time password (OTP). Sometimes, for higher value transactions, the use of a mobile phone is often promoted as the best approach, either by using an SMS or a voice message.

Strong Security

An ideal solution would be a technique that uses strong security and yet is very easy for people to remember how to use both within single channel environments such as web-browsers or for higher value services using a mobile phone as a two channel approach.

Ascertia has licensed GrIDsure® technology within its ADSS GrIDsure Server to provide both strong authentication to access web-sites and strong authorisation to use server-held signing keys so that documents can be digitally signed and secured on behalf of the user.

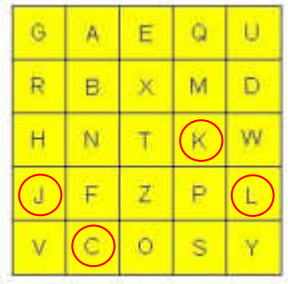
GrIDsure authentication uses a ‘shared secret’ approach. During initial registration a grid is filled with random letters and the user selects a number of squares on a grid that make a memorable pattern or shape, such as a 'tick' or a dispersed pattern. The values create a personal identity pattern or PIP. During subsequent uses the numbers in these PIP locations change each time the grid appears and so the user now observes an efficient and easy-to-use one-time-password generator. It is much easier to use because users find it easy to remember patterns compared with PIN numbers or passwords.

With Ascertia’s ADSS GrIDsure Server users do not need to remember various passwords or questions and answers in their heads, and it’s much more secure since there are so many combinations of possibilities that the chosen memorable pattern is never revealed. This is true even if one or more password entry is observed, key-logged or otherwise captured – these are after all, one-time passwords.

Professor Richard Weber, Churchill Professor of Mathematics at Cambridge University, has concluded that GrIDsure is about 100 times stronger than a password approach.

User Registration

This section presents a typical way in which a user can be registered.

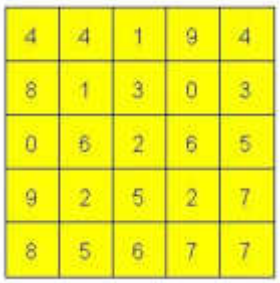


A user can be presented with a registration grid in many ways, including via letter, via a computer screen, a web-browser or via mobile phone. During the registration process the user is identified in some way that suits the business purpose. A random grid of alpha characters is presented to the user. This will typically be a 5x5 grid but there is no technical limit, it is just a size that works well with many non-technical people. They need to choose a memorable PIP of random squares or lines preferably with some diagonal or random content, e.g. JCKL (highlighted in the grid image). This information can be entered into a traditional password field and obscured in the usual manner.

This pattern must be at least 4 characters, 5 is more secure but is slightly harder to remember. Using 4 characters from a 5x5 grid has over 390,000 variations (rather better than ATM terminals with just 10,000 options). Using 5 characters gives almost 10 million variations! You can choose the security level you need.

User Authentication

Now the user is known to the system, they can be challenged at any time and in any way, e.g. on a computer, a terminal, or a mobile phone. All they need to do is enter their userID and the one time password assembled using the digits they see within the challenge grid that match their PIP in both location and order. The challenge grid is always randomly created and usually contains numbers because people feel familiar with these (but it could be other letters or symbols). In a 5x5 grid a number must repeat at least 2 and no more than 3 times for the security to work effectively. So in this example the user will enter a one-time-password of 9567 (check the PIP positions in the grid above with the challenge grid shown here and note that the numbers must be entered in the order that the PIP was registered. Now look at how many combinations of 9567 exist on the challenge grid, in this case it is 54, so it is hard to gain knowledge about what the PIP might be, even if the response is captured. And of course the grid will change every time.



User Authorisation

The user can be repeatedly challenged when important actions are taken. This ensures that others cannot action requests when the logged-on user has walked away from their system. It also stops man-in-the-middle / session take-over attacks from exploiting the user's account. The GrIDsure approach is much simpler and more useable than a hand-held token. It also has considerable value in situations where people have a disability or when users cannot easily protect their PIN, e.g. they have to write it down or they have to say it, simply because the response is only a one-time password and not the memorable PIP itself.

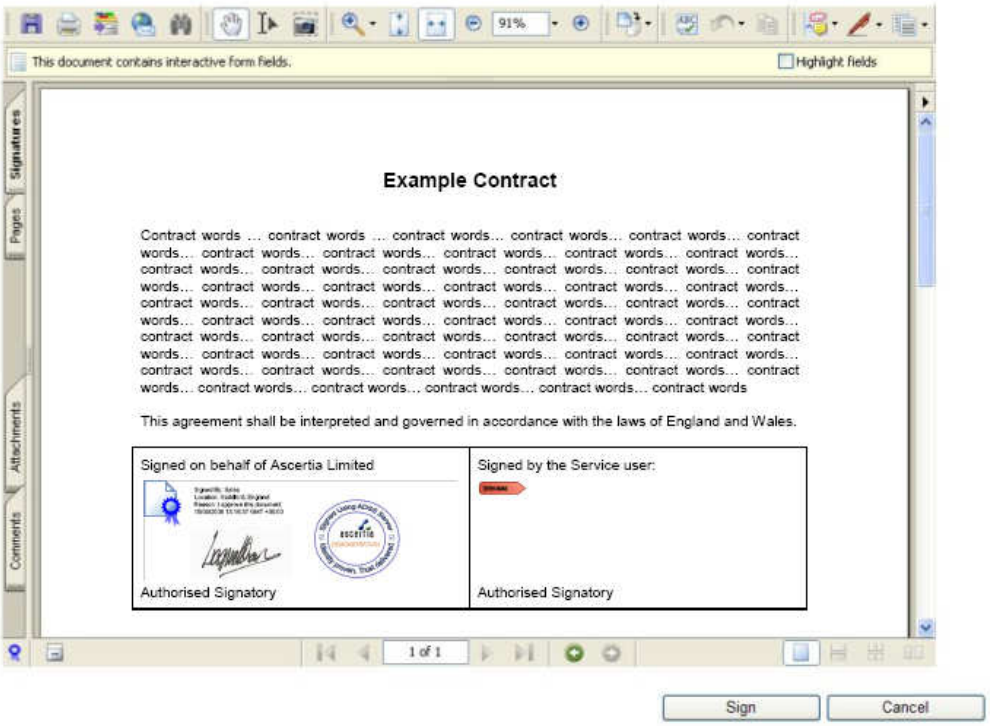
On-line Document Signing

The ADSS GrIDsure Server delivers authentication and authorisation services and thus enables the user to digitally sign business documents. The signing key and digital certificate is generated by the ADSS Server when the user is first registered. The real benefit of using digital signatures is that the data cannot be changed without the signature being subsequently shown as invalid. Without the use of such signatures, electronic data can be changed at will and no-one can be sure whether the data is original, if it was approved or by whom.

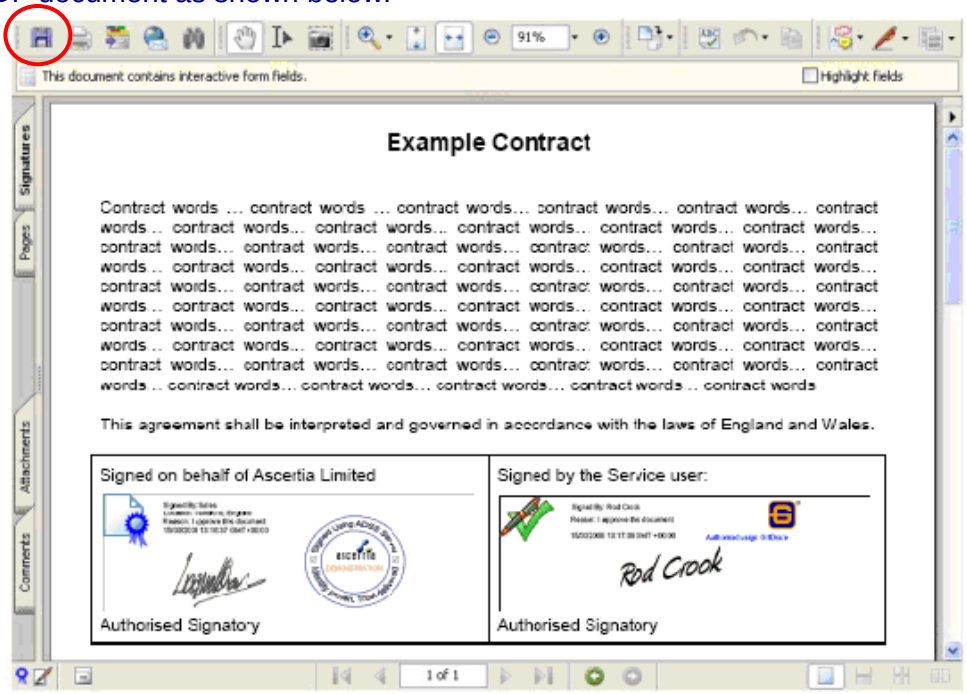
The simplicity of the Ascertia solution is that the user requires no special hardware, software or knowledge and yet the application can simply ask them to confirm that the transaction or document is finished and that they wish to sign and confirm this. The digital signature binds

their identity to the data or document. This approach can be used in an approval workflow. If the organisation also now signs the document then the dual signed agreement can be issued either via the web-browser, e.g. as a PDF document or via email.

The following screen shot illustrates how this can be done. In this scenario, the example PDF contract document has been signed and certified by the business and it is now offered to the service user to sign:



If the user clicks the sign button the signing process is authorised using a GrIDsure challenge process as before. If the user is authenticated then their signing key and certificate are released by the ADSS GrIDsure Server and used to create a digital signature on the PDF document as shown below.



Both parties can now keep a copy of this document. The user can save a copy using the save button (highlighted) or if required the organisation can email a copy to the user. The

document is being shown to the end-user using a well known PDF Reader - this is freely distributed software found on all desktops. Signatures can be verified easily by users by simply clicking on the signature block. Ascertia also provides a server-side signature verification capability.

The process is an example of how the ADSS GrIDsure Server can be used to sign and approve document workflows externally with no need to deploy any signing software to the users or hardware tokens or issuing of any digital certificates to users. The end-user keys can be protected in centrally-held Hardware Security Modules (HSMs) so that there is no danger of this data being exposed, even by trusted staff.

Using this approach trust services can be cheaply and easily delivered to everyone. Any organisation that has registered end-users with an effective Know-Your-Customer process can use this approach. The Ascertia ADSS Server can issue certificates under an organisational Root CA and Issuer CA. During registration links with credit reference agencies can also be made to seek external confirmation of user identity that are good enough to be used for high assurance certificates. For internal users the background check can be made against company's HR systems. Should links with commercial CAs be required then automated registration and certificate issuance can also be easily implemented.

Examples Uses

ADSS GrIDsure Server technology can be applied to any business use. e-Commerce sites typically use multiple web-form interactions with an end-user to complete a set of transactions. These details should be summarised into a PDF document and then digitally signed. As shown before the presence of a hand-signature impression makes people feel much more comfortable that they are looking at a signature – rather like printed signatures seen on many company letters these days – even though the security is related to the actual embedded digital signature.

Documents with digital signature have legal standing and signed credit agreements attract a higher value when sold on to other financial services organisations. It is also clear that insurance quotations can be confirmed and policies issued with digital signatures saving millions of pounds in paper and postage every year.

Using this system orders can be placed, agreements created, contract notes issued, credit arrangements agreed, financial instructions confirmed and receipts issued - the possibilities for e-business are endless!

Summary

Ascertia's ADSS GrIDsure Server enables business applications to use strong authentication and strong authorisation options. By using digital signatures organisations can create legal weight evidence to reduce errors, reduce the legislative and regulatory risks, as well as substantially reduce the paper and fraud costs of e-business.

Ask Ascertia for further information on how to deliver trust within your business documents and workflow process info@ascertia.com

Identity Proven, Trust Delivered