INgrid is a revolutionary authentication technology that takes advantage of the natural human ability to remember patterns and shapes. Through the use of patterns, PINgrid is able to ensure that secret information is kept in your head and can’t be compromised. The result is a highly secure yet simple-to-use logon system which removes the need for users to carry dedicated hardware tokens or remember multiple passwords or PINs.

Using PINgrid is incredibly simple, as many of us do this sort of thing every day without even realising it: every time you unlock your phone or use an ATM, do you actually look at the numbers or just press the buttons in a remembered pattern or sequence?

How it works
With PINgrid you only ever need to remember a pattern - not a number, alphanumeric string or any sort of password. At logon, you are presented with a grid of ‘random’ numbers. By overlaying your secret pattern onto the grid you will ‘see’ your passcode. Since all the numbers change every minute, a new passcode is also created even though the pattern stays the same.

The grid can be displayed within an application or on a web logon page for 1.5 factor authentication, or on a smart phone via a soft token app, email or SMS for full 2 factor authentication.

As the secret pattern never leaves your mind it can’t be compromised by malware, key logged or even shoulder surfed. Furthermore, the something you know is combined with the ‘something you have’ to produce the One Time Code so the individual factors cannot be separated, attacked or reverse-engineered.

Features and highlights
• NO hardware tokens!
• Securely logon on to Windows Desktops while in or out of the office
• Native transaction signing / validation capabilities.
• Emergency Override Access
• Secure access to internal & Cloud-based applications
• Highly competitive pricing and flexible licencing options.
• 1.5 and 2 factor authentication
• Free Soft Token download from all major mobile app stores
• Real-Time or Pre-Send token delivery via SMS or email
• Active Directory or LDAP database storage (no schema extensions)
• RADIUS & Web Services interface for universal integration
• Rapid user provisioning (thousands in an hour)
• Web-based Operator portal for help-desk day-to-day operations
• Self-service password reset
• FIPS 198 & 180-3 compliant
• Patent-pending technology

www.winfrasoft.com
INgrid fuses ‘something you have’, ‘something you know’ and ‘something you are doing’ to produce an OTP rendering the elements inseparable to exponentially increase logon and transaction security.

Traditional 2 Factor vs. PINgrid 2 Factor
Traditional 2 factor authentication is based on ‘something you have’ (a token) and ‘something you know’ (a PIN or password) which is supposed to help identify a user. With traditional systems the ‘something you have’ can be used by anybody who has it, not just its intended owner, and the ‘something you know’ (like a 4 digit PIN) can easily be stolen when you type it in (think ‘keystroke logger’). Furthermore, there is no way to prove your intentions.

With PINgrid, the ‘something you have’ (the grid) can only be used by you and is of no use to anybody else even if they got hold of it. The ‘something you know’ (the pattern) is never divulged and remains private during the logon process. Transaction specific information can easily be entered into the soft token to prove your intentions and prevent man-in-the-middle attacks.

Hardware vs. Software tokens
With many companies using some form of hardware based token, users are getting increasingly frustrated at the complexity and lack of convenience of logging in, especially when using mobile device and tablets. In these environments security is viewed as a blocker to getting on with the day job.

In contrast, PINgrid does not require the user to carry around anything extra. Most people already have a mobile device with them at all times, which suits the newly mobile workforce - importantly they realise very quickly when they don’t! This changes the perception of security from cumbersome to convenient.

The frustration with traditional tokens, combined with the emergence of “Risk Appropriate Authentication” calls for a more granular solution. PINgrid provides this with its 1.5 and 2 factor authentication options, endpoint independence and transaction signing capabilities. Companies can now determine the risk of a user’s activity and allocate the appropriate authentication method; for instance Internet Banking could use 1.5 FA logon for read-only purposes followed by 2 FA with transaction signing to authorise a payment.

Weak signal, no data, flat battery... no problem
PINgrid’s variety of token types are designed to handle just about every eventuality. The soft token is an entirely off-line app which does not require signal or data connectivity, and will work just fine in an underground bunker or while roaming internationally (without the data charges). A user can have up to 10 registered devices at a time using a single licence for greater flexibility.

SMS and email delivery options are also available. Real-time delivery requires connectivity, but tokens are only sent when needed, whereas Pre-Send delivery ensures users have a token waiting when they need it.

PINgrid soft tokens are available on all major app stores as well as for Windows XP and higher PCs.