The Titan Key Revenue and Productivity Model for ISPs

Version 1.1

October 18, 2003

The Titan Key's goals for ISPs

The founders of TitanKey Software were principals in a commercial ISP operation from 1994 to 2001. Their difficulties and frustrations in dealing with spam led to the creation of The Titan Key. Their background in the ISP business dictated that the primary beneficiaries of the product should be the ISP. The resulting requirements for the product included:

- **Reduce Customer Churn.** Too many customers are switching ISPs just to get away from the spam.
- **Eliminate Wasted Bandwidth.** The ISP is forced to carry content that customers loathe, much less willing to pay for.
- **Minimal impact on staff.** The last thing an ISP needs is a technology that increases overhead or requires significant training. Subscribers should be able to provision and maintain their own anti-spam service.
- **Generate Revenue.** In addition to all of the above, the product must also generate revenue for the ISP.

The Titan Key directly addresses all of these issues with a powerful yet simple product. The relevant features are highlighted below.

Customer loyalty is *rewarded*

The Titan Key shatters the loyalty dis-incentive that spam has created Many customers to switch ISPs just to rid themselves of spam. The "no such user" or "hard bounce" error message that The Titan Key returns to mass-email software typically directs it to flag the email address for deactivation or removal from the database. Email addresses that continually fail due to hard bounces are eventually no longer used because invalid email addresses waste processing time and are worthless to a spammer. The sheer volume of spammer databases require that they eliminate email addresses that no longer function.

The net result to a user of The Titan Key is that over time, their email address will be on fewer spammer databases.

This is a 180 degree reversal of the previous trend. The benefit to ISPs is significant. Because The Titan Key dynamically builds a database of "known senders" while at the same time it blocks spammers and reverses propagation of their email address on spammer databases, *customer ISP subscriptions become more valuable over time.* Unlike traditional anti-spam approaches, The Titan Key rewards customer loyalty by strengthening the subscriber's privacy capabilities over time.

Spammers cannot send spam

Because The Titan Key user's email address literally does not work for spammers, by definition of the SMTP standards, *they cannot even send the spam.* No other software can make this claim.

Network bandwidth is liberated

Because spam cannot be sent, all of the network bandwidth that was previously wasted is now available for productive use. For the ISP, the savings are significant. Close to 50% of today's email is spam.

Transparent Installation

The Titan Key installs as the primary MTA. It can be installed as a hardware network appliance using a dedicated server or array of servers or it can be installed as a software service on an existing Windows-compatible server.

The default operation of The Titan Key is to transparently pass all email that does not have a valid subscriber account. This means that on day one of the installation, there is no impact on the subscriber base or the network. All email (including spam) passes through.

Only when subscribers self-provision the service does The Titan Key begin protecting *their email address only*. All other subscribers remain unaffected. There are many benefits to this approach which are highlighted below in self-provisioning.

The transparent installation qualities of The Titan Key allow ISPs to install and test the product with minimal impact. When combined with the built-in fail safe and self-healing qualities of SMTP, the installation risks to the organization are minimized.

Self-serve provisioning

Once The Titan Key has been properly installed, the subscriber is given a URL where they can provision their service. There is nothing else for the ISP to do. The user authenticates against their existing email address and POP3 password (see Integrated Authentication below) and proceeds through a checklisted interface that walks them through their installation process which includes:

- Initial setup and personalization
- Transfer of any existing "known senders". Any text file of email addresses can be uploaded or the user can run an included utility to extract email addresses from any Outlook folder. This seeds their database so that unnecessary invite/verify processes to known senders are minimized.
- Running The Titan Key in "passive" mode, allowing the user to see how The Titan Key will treat a given email without actually rejecting it. Email from a sender that is not on the list of "known senders" will have "[unknown]" inserted in the Subject line. The user can then fine-tune The Titan Key as needed.
- Running The Titan Key in "active" mode, using the complete email rejection capability. Once the user turns on "Active" mode, they will never receive spam again.

Self-provisioning gives the user complete control of how and when they want to use The Titan Key's features without having to burden support or administrative staff. The ISP has complete freedom in how the service is to be offered, how much will be charged, and when.

Integrated Authentication

Today's user has to either remember or maintain an excessive list of usernames and passwords. The Titan Key does not add to that list. Instead, it simply uses the user's email address and POP3 server password to provision and authenticate their access. This allows the ISP to use existing helpdesk databases to respond to customer support requests to reset their passwords if necessary. And because there is no local storage of passwords, any changes made to the POP3 server accounts are instantly used by The Titan Key logon process.

Automated maintenance

Only typical hardware, O/S, and database server maintenance is required by the ISP. All other functions are handled automatically by a daily process, including:

- Daily subscriber "dashboard" reports that detail various activity such as unknown sender attempts, validated users, and VPM usage.
- Database purges of invalidated, unknown users that have not validated themselves after 30 days.
- Weekly XML subscriber activity reports to the ISP to be used for billing purposes.
- Removal of subscriber accounts that have not existed for over 30 days.

The automated maintenance features of The Titan Key keep administrative overhead to a minimum. For the most part, only standard hardware, O/S, and database low-level maintenance is required and is most likely already a solid part of the ISPs skillset.

Minimized ISP censorship liabilities

Customers that elect to use The Titan Key are the *only* ones that decide what email they block and what they receive. Because there are no other parties that influence this censorship in any way, the ISP's liability for censoring spam is minimized. This feature does not construe legal advice and it is highly suggested you consult with your attorney as to the actual legal effectiveness of our claims.

Your subscribers cannot claim their ISP is inappropriately blocking email simply because *they* are the ones blocking the email.

Summary

We believe The Titan Key is the only solution that gives ISPs a complete solution to the root of their problems.

- **Customer Churn is Reduced.** The Titan Key's operation rewards customer loyalty by strengthening their privacy protection and reducing propagation of their email address to unauthorized databases over time.
- **Bandwidth Waste is Eliminated.** Because The Titan Key stops spam before it is ever sent, spam bandwidth is reduced to zero *across the entire Internet.*
- **Staff impact is minimized.** The Titan Key's integrated authentication, self-service provisioning and automated maintenance reduces administrative overhead to the lowest possible levels.

- **Revenue is Generated.** Because The Titan Key can be offered as an optional service and integrated with the ISP's provisioning system, a nominal charge can be levied to the user that gives them the best spam protection on the market at the lowest price.

The Titan Key was designed by an ISP for ISPs. The lofty goals were met via a deep understanding of the SMTP protocol and genuine out-of-the-box thinking. The result is a revolutionary product that both solves the ISP's woes while giving the community a technology that actually has a chance at truly eliminating the spam problem.

We urge you to visit the Web site *right now* at www.titankey.com for a complete demo and contact TitanKey Software to begin implementation planning.