WHAT IS CLAIMED IS:

1. A computer-implemented method for conducting a transaction, comprising:

receiving, by a thin client from a portable device of a first portable device type, transaction data;

determining, by the thin client, that the portable device is the first portable device type based on the format or content of the transaction data;

applying, by the thin client, an encryption protocol associated with a second portable device type to the transaction data to create encrypted data, wherein the encryption protocol is applied based at least in part on determining that the portable device is the first portable device type; and

transmitting, by the thin client to a remote computer, the encrypted data, wherein the remote computer utilizes the encryption protocol to decrypt the transaction data, and thereafter processes the transaction data to conduct the transaction.

2. The computer-implemented method of claim 1, wherein the thin client is operated by a resource provider.

3. The computer-implemented method of claim 1, wherein the remote computer provides access device transaction functionality as a service.

4. The computer-implemented method of claim 1, further comprising establishing a secure channel between the thin client and the remote computer, wherein the encrypted data is transmitted over the secure channel.

5. The computer-implemented method of claim 4, wherein establishing the secure channel further comprises:

generating, by the thin client, an ephemeral key pair comprising an ephemeral private key and an ephemeral public key;

generating, by the thin client, a random value;

generating, by the thin client, a concatenated value comprising the ephemeral public key and the random value;

digitally signing, by the thin client, the concatenated value with an authentication private key associated with the thin client; and

transmitting, by the thin client to the remote computer, the concatenated value as digitally signed.

6. The computer-implemented method of claim 1, further comprising:

receiving, by the thin client from the remote computer, subsequent encrypted data, wherein the thin client is configured to decrypt the subsequent encrypted data utilizing the encryption protocol; and

verifying, by the thin client, the subsequent encrypted data is unaltered and was transmitted by the remote computer.

7. The computer-implemented method of claim 1, further comprising:

generating, by the thin client, a secure communications wrapper, wherein the encrypted data is generated utilizing the transaction data and the secure communications wrapper.

8. The computer-implemented method of claim 1, wherein the encryption protocol is unknown to portable devices of the first portable device type.

9. A thin client comprising:

a processor; and

a computer readable medium coupled to the processor, the computer readable medium comprising code that, when executed by the processor, causes the thin client to:

receive, from a portable device of a first portable device type, transaction data associated with conducting a transaction;

determine that the portable device is the first portable device type based on the format or content of the transaction data;

apply an encryption protocol associated with a second portable device type to the transaction data to create encrypted data, wherein the encryption protocol is applied based at least in part on determining that the portable device is the first portable device type; and

transmit, to a remote computer, the encrypted data, wherein the remote computer utilizes the encryption protocol to decrypt the transaction data, and thereafter processes the transaction data to perform the transaction.

10. The thin client of claim 9, wherein the thin client is operated by a resource provider.

11. The thin client of claim 9, wherein the remote computer provides access device transaction functionality as a service.

12. The thin client of claim 9, wherein executing the code further causes the thin client to establish a secure channel between the thin client and the remote computer, wherein the encrypted data is transmitted over the secure channel.

13. The thin client of claim 12, wherein establishing the secure channel further causes the thin client to:

generate an ephemeral key pair comprising an ephemeral private key and an ephemeral public key;

generate a random value;

generate a concatenated value comprising the ephemeral public key and the random value;

digitally sign the concatenated value with an authentication private key associated with the thin client; and

transmit, to the remote computer, the concatenated value as digitally signed.

14. The thin client of claim 9, wherein executing the code further causes the thin client to:

receive, from the remote computer, subsequent encrypted data, wherein the thin client is configured to decrypt the subsequent encrypted data utilizing the encryption protocol; and

verify the subsequent encrypted data is unaltered and was transmitted by the remote computer.

15. The thin client of claim 9, wherein executing the code further causes the thin client to generate a secure communications wrapper, wherein the encrypted data is generated utilizing the transaction data and the secure communications wrapper.

16. The thin client of claim 9, wherein the encryption protocol is unknown to portable devices of the first portable device type.